Microsoft Azure

From Zero to Hero
The Complete Guide

Memi Lavi
www.memilavi.com

Why Cloud?

90% of software companies use the cloud

The world is going to the cloud

Don't get left behind!

for cloud services

Why Microsoft Azure?

The 2nd largest public cloud

MONSTER

azure Jobs (15565 Jobs Found)

The most popular in enterprises

Note

You don't have to know ANYTHING about cloud

You don't have to know ANYTHING about Azure

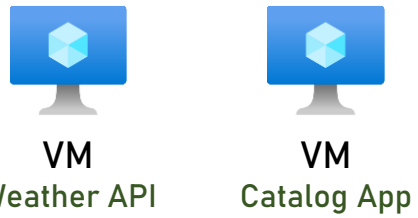
We're going to learn everything from the start

We're going to have a lot of Azure hands-on

We'll go from here…

ReadIt!

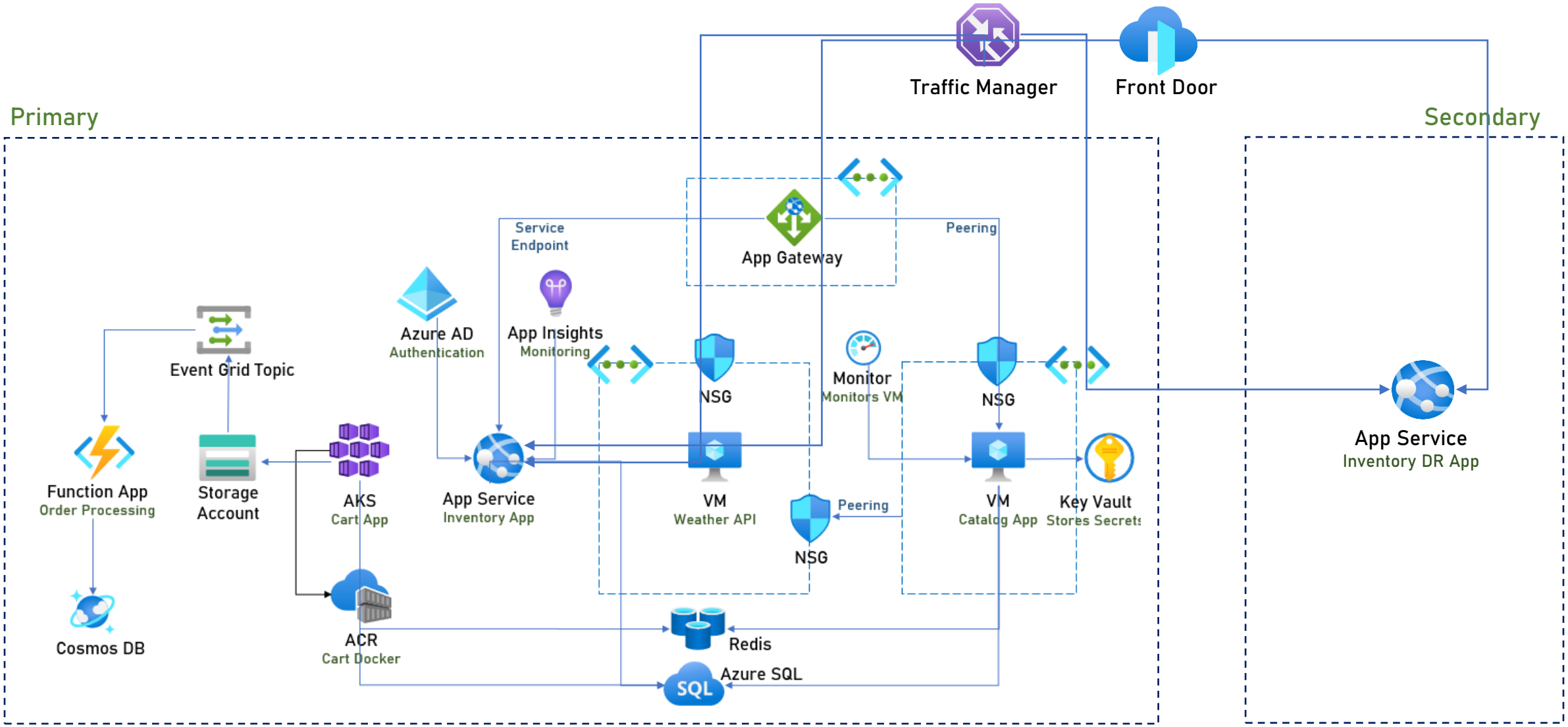
Cloud Architecture



To here…

ReadIt!

Cloud Architecture



By the End of This Course…

- You'll know what is the cloud
- You'll know what is Azure
- You'll know what you can do with it
- You'll learn how to use its services
- You'll learn how to design modern, secure, reliable apps
- You'll become a Cloud Architect!

This Course Is Different

- Very practical
- Extremely hands-on
- Emphasis on what you'll actually use

But That's Not All...

At the end of this course -

Download the Azure Architecture Summary!

The ultimate, practical, guide to help you design great cloud architecture!

Who Am I?

Senior Software & Cloud Architect

Memi Lavi
www.memilavi.com

My Clients

Microsoft

DXC.technology

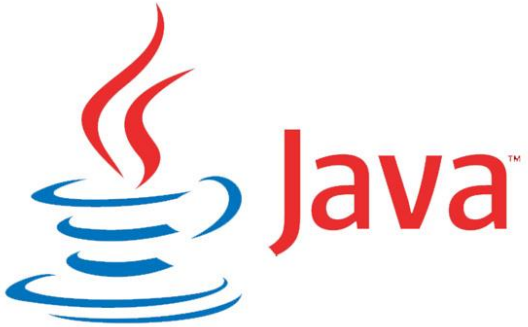
Hewlett Packard
Enterprise

ForeScout®

IAI

DOCOMOTION
INTERACTIVE DOCUMENTS

My Technology Stack



Azure Certified

Speaker

NORDIC APIS

Memi Lavi
Polar Technologies

DEVOXX™ GREECE

DevDays

BUY TICKETS

Venue

Memi Lavi

Independent Consultant, Israel

Who Is This Course For?

- Architects and Architects to be
- Developers who want to learn about the cloud
- Anyone who is interested in the most important computing platform in the world

How This Course Is Organized

Overview of the cloud and Azure

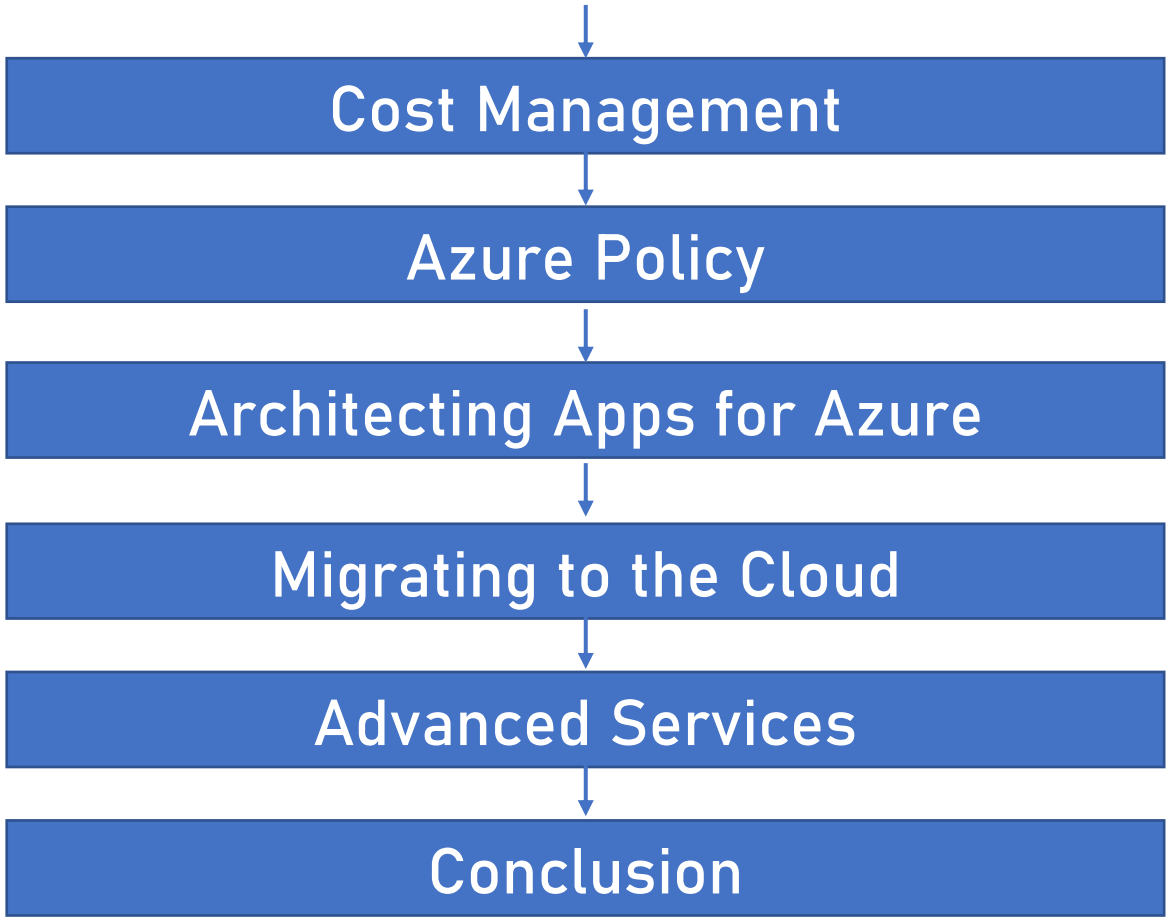
Overview of main services (demos + hands on)

Architecting modern apps on Azure

Agenda

- Welcome
- Introduction to the Cloud
- Introduction to Azure
- First Look at Azure
- Basic Concepts
- Introducing Our App
- Compute
- Networking
- Data
- Messaging
- Azure Active Directory
- Monitoring
- Security
- DR

Agenda


Cost Management
Azure Policy
Architecting Apps for Azure
Migrating to the Cloud
Advanced Services
Conclusion

Introduction to the Cloud

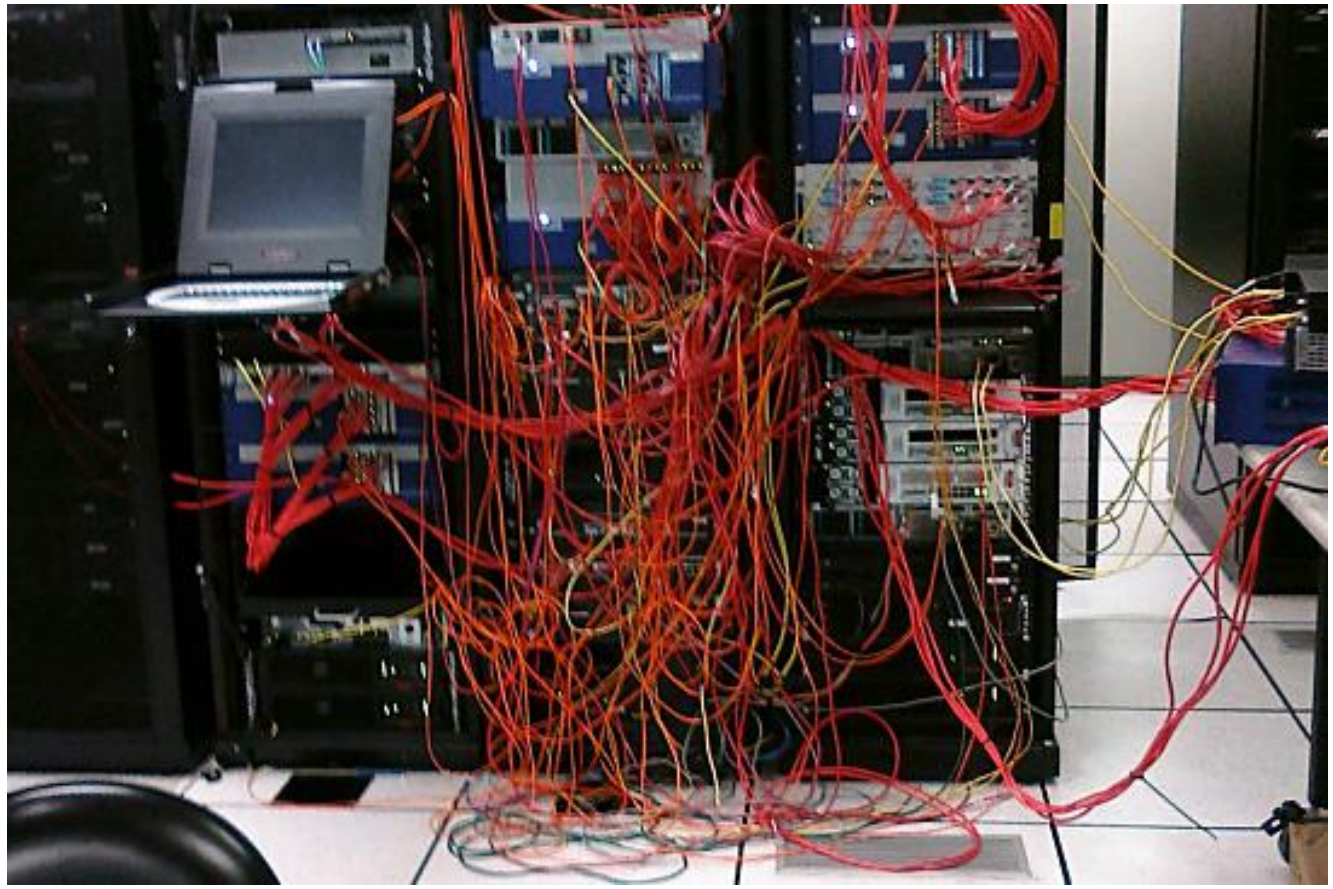
Memi Lavi
www.memilavi.com

Before the cloud…

- If you needed a server, you had to:
  - Buy it
  - Install it
  - Maintain it
  - Replace it
  - Have an IT team

Before the cloud…

- You often ended up with this:



Before the cloud…

- The same goes with:
  - Networking
  - Databases
  - User Management
  - And more…

Before the cloud…

- But there's more…

BLACK FRIDAY

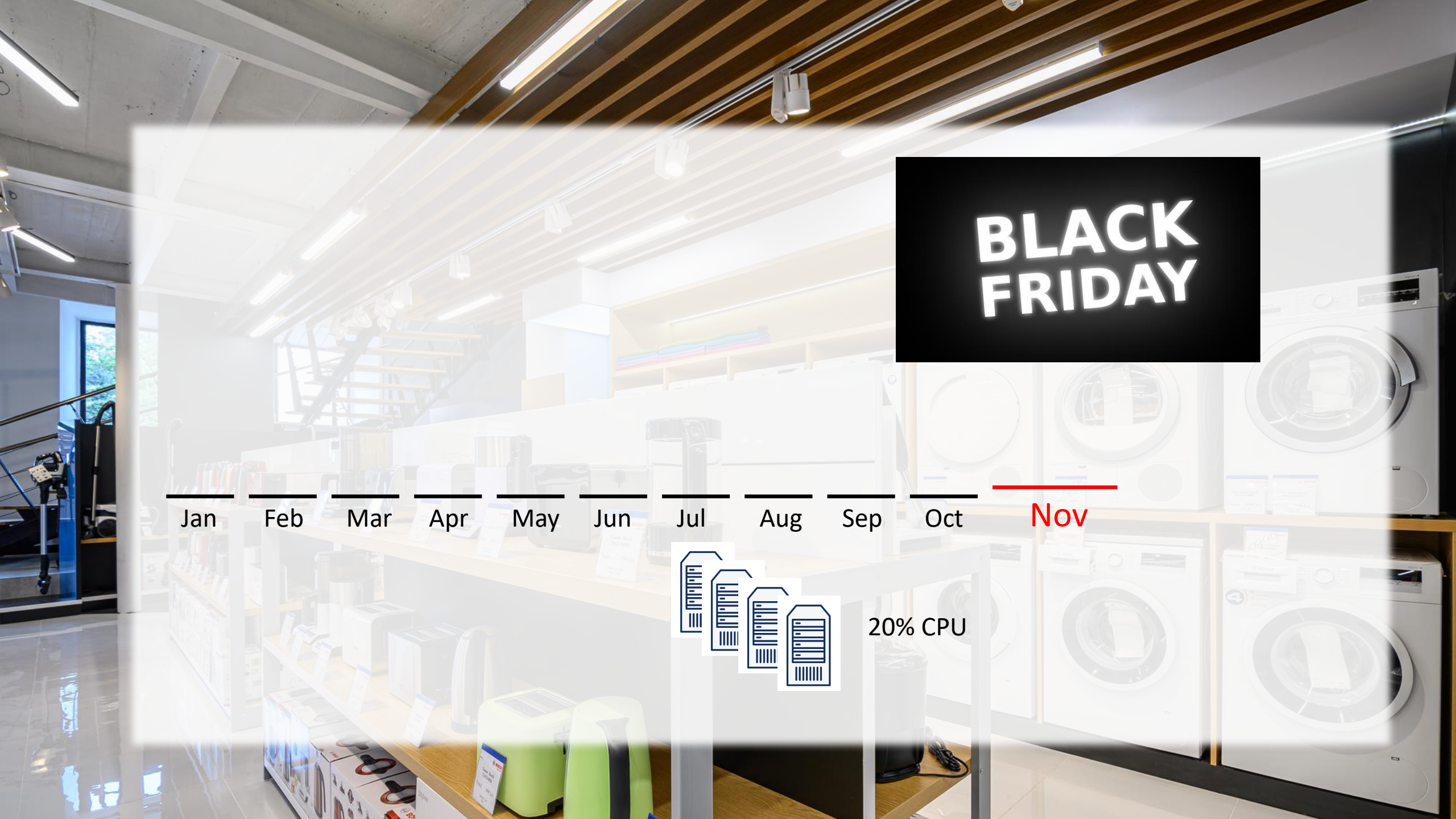
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov

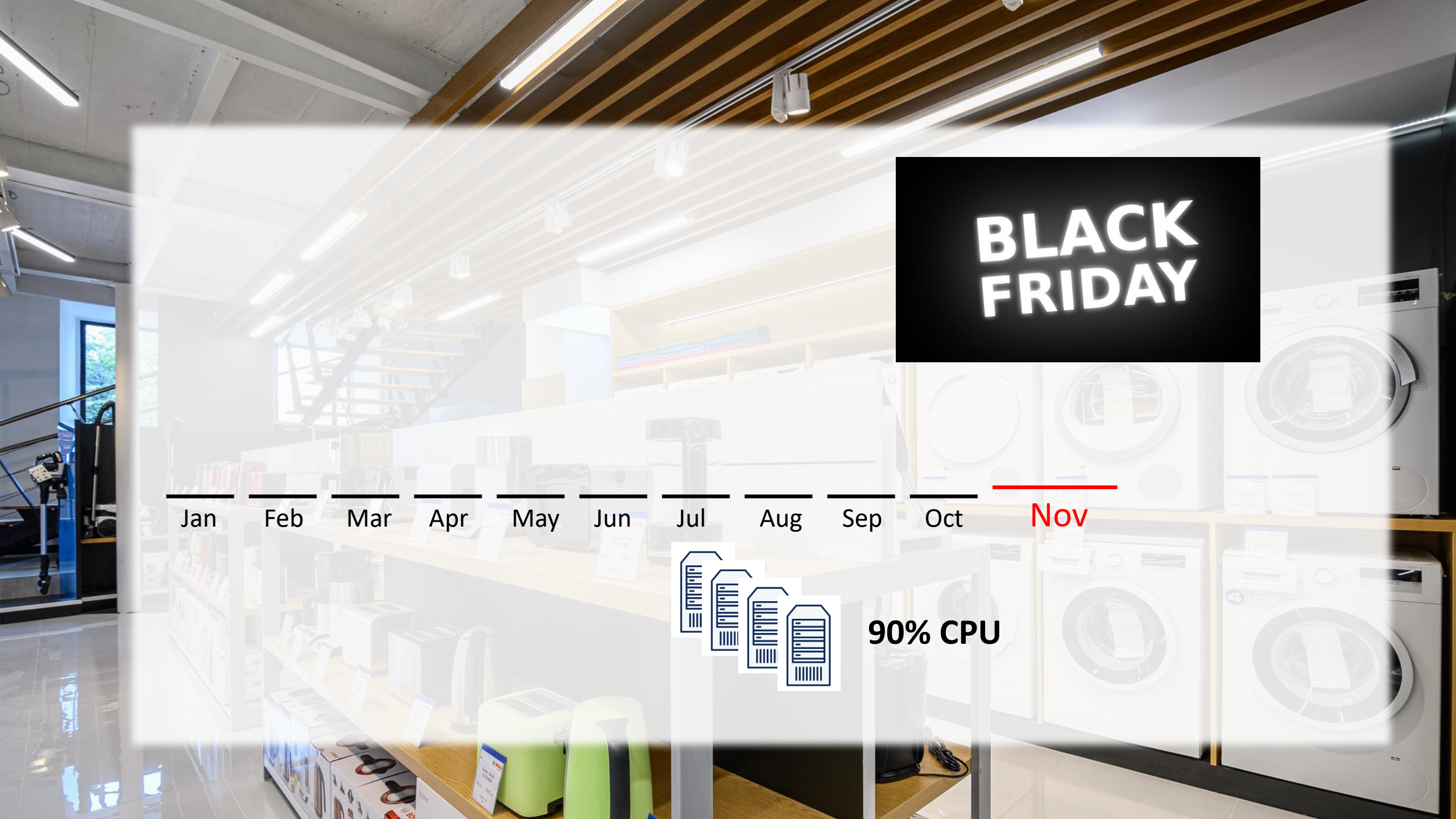
60% CPU

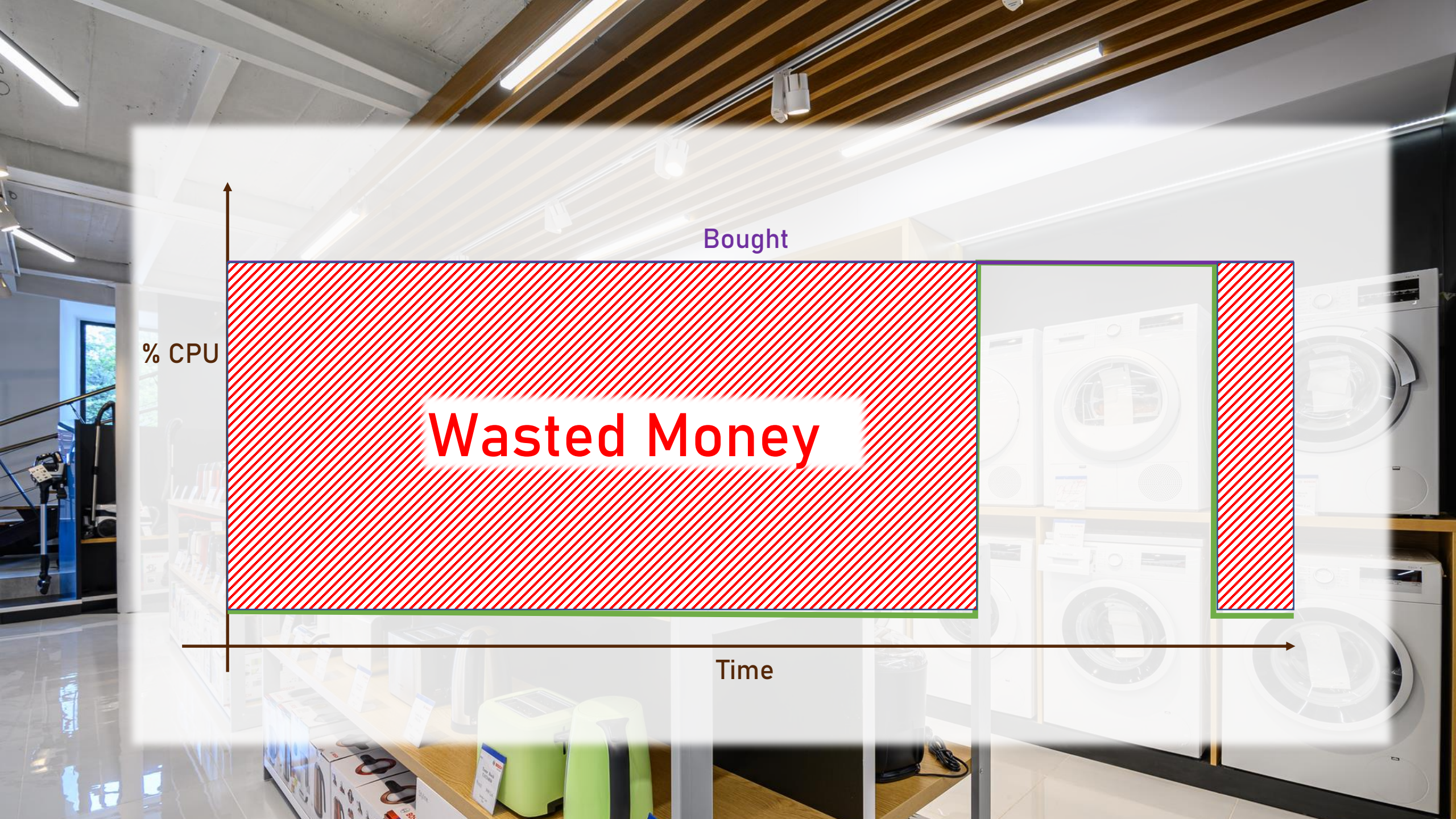
BLACK FRIDAY

Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov

120% CPU

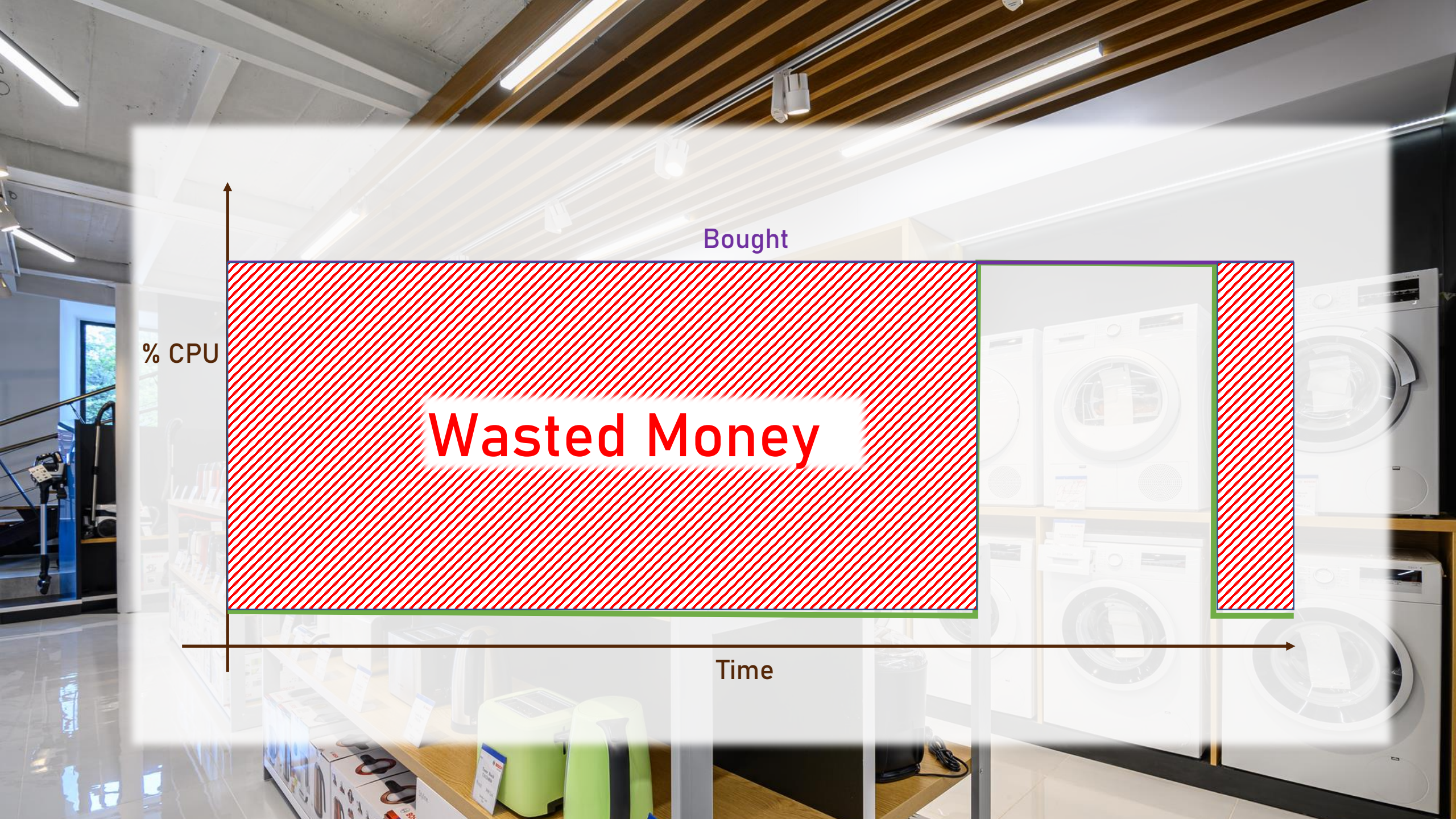

BLACK
FRIDAY
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
20% CPU


BLACK
FRIDAY
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
90% CPU


Bought
% CPU
Wasted Money
Time

Before the cloud…

- If you needed a server, you had to:
  - Buy it
  - Install it
  - Maintain it
  - Replace it
  - Have an IT team


Bought
% CPU
Wasted Money
Time

The Cloud:

Compute, Networking, Storage and other services

Managed by SOMEONE ELSE

Cloud Providers

- Companies who build huge data centers
- Fill it with servers, networking, cooling, electricity etc.
- Design and install various services
- Make it publicly accessible

Data Center

Microsoft Azure Datacenter in Washington

Data Center

Microsoft Azure Datacenter in The Netherlands

Cloud Services

- Clouds are huge and the competition is fierce
- Offer a lot of additional services:
  - AI
  - IOT
  - Kubernetes
  - And lots more…

In the cloud era…

- If you need a server, you can:
  - Create it in the cloud within minutes
  - Use it as you wish
  - Pay for what you use
  - Shut it down when not needed
  - Automatically maintained, patched, secured, monitored

The Cloud:

Compute, Networking, Storage and other services

Managed by SOMEONE ELSE

5 Characteristics of Cloud Computing

On-Demand Self Service

Broad Network Access

Resource Pooling

Rapid Elasticity

Measured Service

On-Demand Self Service

- No human interaction is needed for resource provisioning
- Resource can be provisioned (created) with a click of a button
- Provisioning is available 24/7

Broad Network Access

- Resources can be accessed from anywhere using the network
- Ideally high broadband
- No physical access is required at any time

Resource Pooling

- Physical resources are shared between customers
- The cloud's backbone decides which physical resource to allocate for a customer's virtual services
- Some advanced cloud services allow for physical resource separation

Rapid Elasticity

- Resources can be scaled up and down as needed, automatically
- No need to purchase resources for a one-time peak scenario

Measured Service

- Payment is done only for resources actually used
- Server time / DB storage / Function calls etc.
- Measurement usually done in high-resolution
  - Server time by the second
- No need to invest money in non-used resources

CapEx

Capital Expense

Making upfront investment for future use / profit

OpEx

Operating Expense

Pay for what you actually use

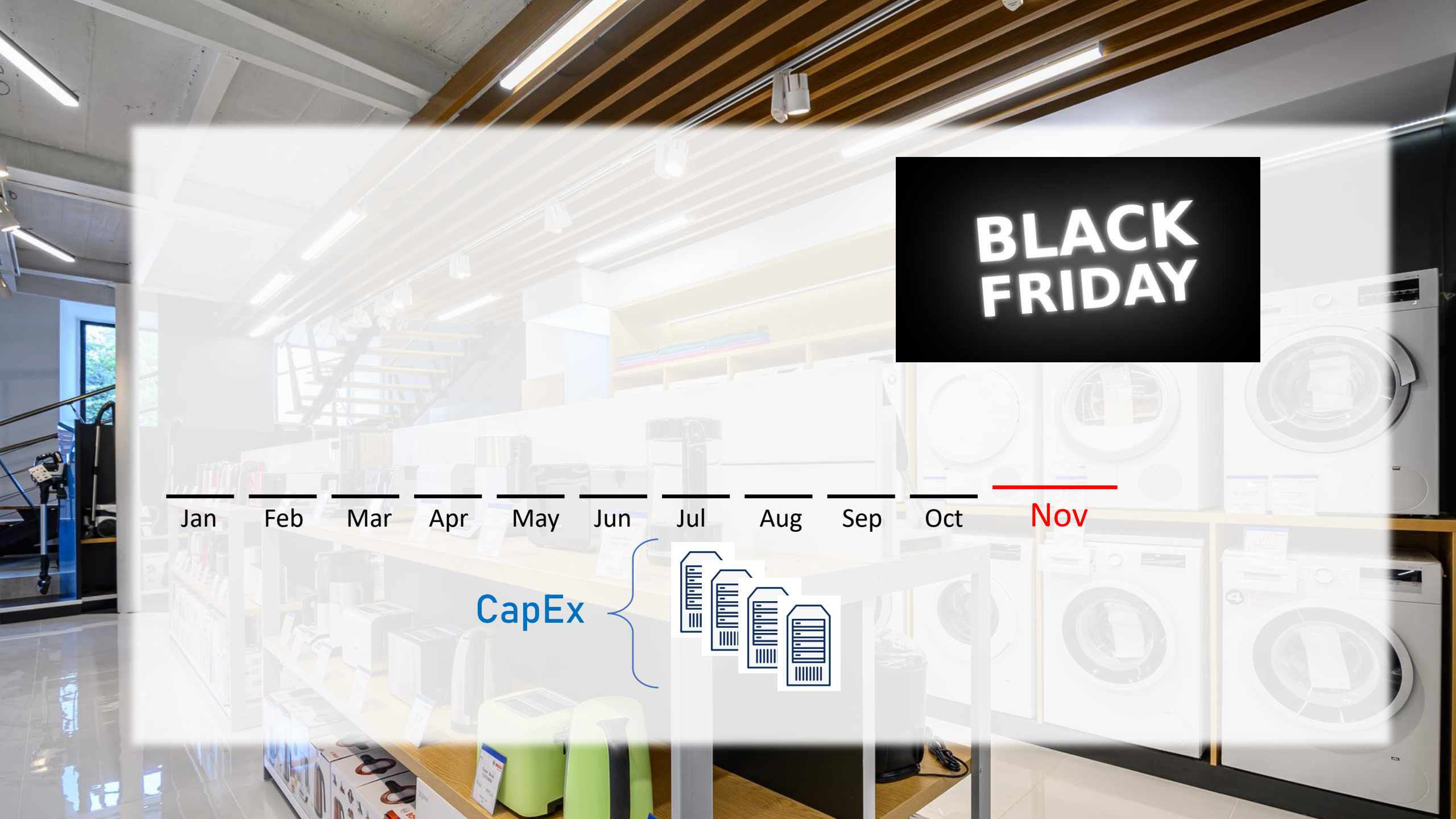
Traditional IT – CapEx Oriented

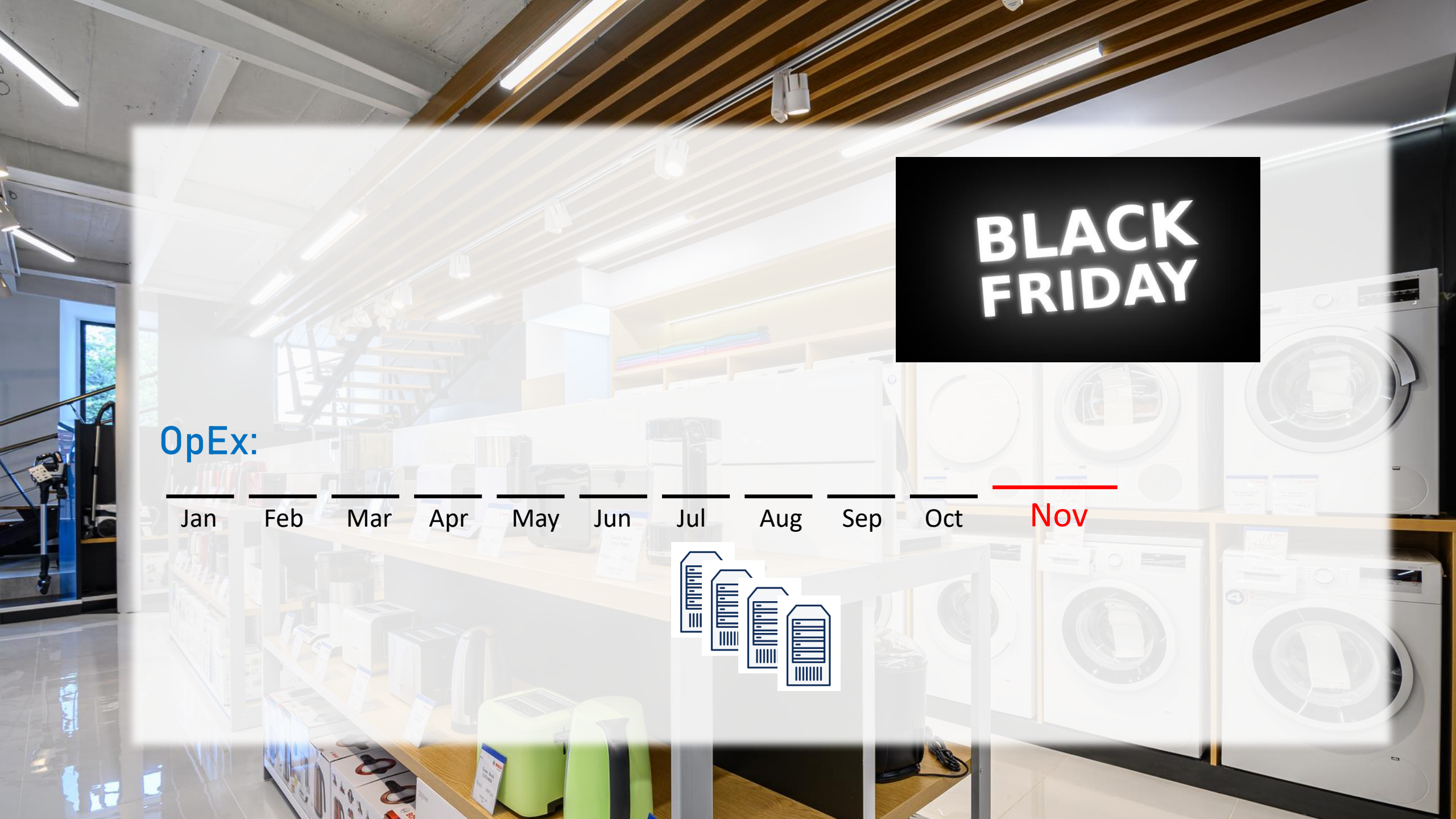
- Major investment for:
  - Building data center
  - Purchasing servers
  - Purchasing air conditioning
  - Purchasing network devices
  - Purchasing software licenses (DB etc.)

…And only then – it can be used…

Traditional IT – CapEx Oriented

- There's also OpEx involved:
  - Electricity
  - Salaries
  - Maintenance
  - And more…


BLACK FRIDAY
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
CapEx


BLACK
FRIDAY
OpEx:
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov

CapEx

Capital Expense

Making upfront investment for future use / profit

- Non optimal
- Not flexible

This is what you get with the cloud →

OpEx

Operating Expense

Pay for what you actually use

- Extremely flexible
- Most optimal

Types of Cloud Services

IaaS

PaaS

SaaS

IaaS

- Infrastructure as a Service
- The cloud provides the underlying platform
  - Compute
  - Networking
  - Storage
- The client handles, and is responsible for all the rest

IaaS

- Most common example:
  - Virtual Machines
- The cloud provides the host machine, networking and disks
- The client creates the virtual (guest) machine, installs software on it, patches it, maintains it etc.

PaaS

- Platform as a Service
- The cloud provides platform for running apps
- Including: Compute, networking, storage, runtime environment, scaling, redundancy, security, updates, patching, maintenance etc.
- The client just needs to bring the code to run

PaaS

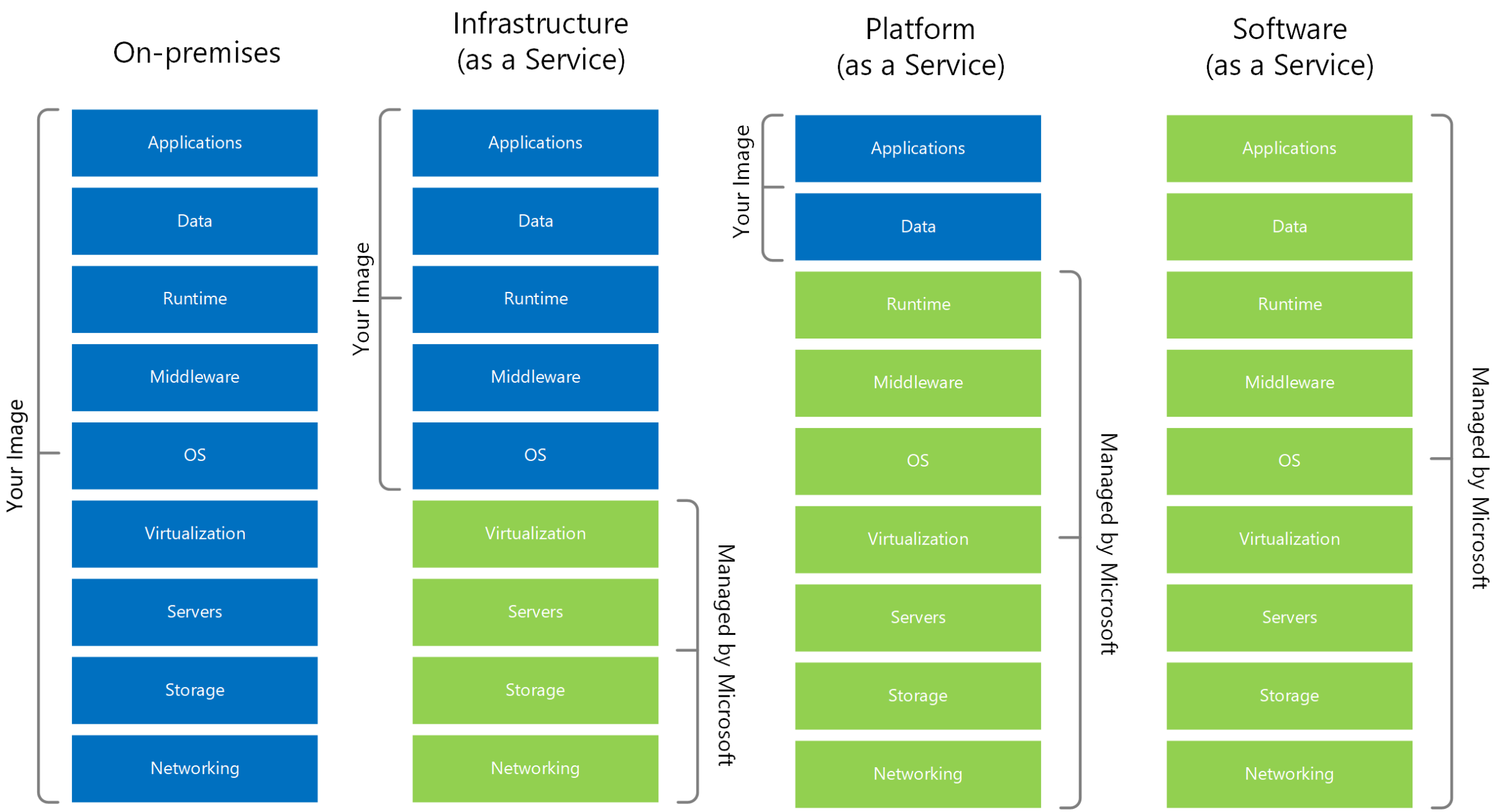
- Most common example:
  - Web Apps
- The cloud provides the runtime for running web apps
- The client uploads the code, and it just runs
- The client has no access to the underlying virtual machines

SaaS

- Software as a Service
- A software running completely in the cloud
- The user doesn't need to install anything on-premises or on his machine
- The provider of the software takes care of updates, patches, redundancy, scalability etc.

SaaS

- Common examples:



Source: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/strategy/monitoring-strategy

Additional Service Types

- FaaS – Functions as a Service
- DBaaS – Database as a Service
- DaaS – Desktop as a Service
- IOTaaS – IOT as a Service
- AIaaS – AI as a Service

Types of Clouds

Public

Private

Hybrid

Public Cloud

- The cloud is set up in the public network
- Managed by large companies
- Accessible through the internet
- Available to all clients and users
- Clients have no access to underlying infrastructure

Public Cloud

Private Cloud

- A cloud set up in an organization's premises
- Managed by the organization's IT team
- Accessible only in the organization's network
- Available to users from the organizations
- Uses private cloud infrastructure and engines
- Contains a subset of the public cloud's capabilities

Private Cloud

vmware CLOUD™

RED HAT® OPENSHIFT Container Platform

Azure Stack

Hybrid Cloud

- A cloud set up in an organization's premises…
- …but also connected to the public cloud
- Workload can be separated between the two clouds
- ie. Sensitive data in the organization's premises, public data in the public cloud
- Usually managed by the public cloud, but not always

Hybrid Cloud

We're going to talk about…

Public

Private

Hybrid

Cloud Providers

- Companies which build datacenters and provide public cloud services
  - IaaS, PaaS, SaaS
  - Other services

Main Cloud Providers

Magic Quadrant

Figure 1: Magic Quadrant for Cloud Infrastructure and Platform Services

Cloud Providers Growth

Q3 2023:

Cloud	% Growth
AWS	12%
Azure	29%
Google	24%

Azure is the fastest growing public cloud, for years

Introduction to Microsoft Azure

Memi Lavi
www.memilavi.com

- Microsoft's public cloud
- Announced in October 2008
- Released in February 2010
- The 2nd largest public cloud
- Closing the gap…

- First focused on PaaS services
  - To counter AWS's IaaS focus
- Later added IaaS
- Currently offers the largest variety of cloud services

Azure

- Major clients:

BOEING

ebay

SAMSUNG

BMW

Regions

- Microsoft built a lot of datacenters for Azure
- Each datacenters' location is called Region
- There are ~60 Azure Regions (more than any other cloud)
- Almost every new resource in the cloud should be allocated to a region

Source: https://azure.microsoft.com/en-us/global-infrastructure/geographies/

Zones

- Some of the regions have more than one physical datacenter
- Great for availability in case one datacenter fails
- Each datacenter is called Zone
- When there are more than one datacenter in a region, the region is said to have Availability Zones
- Some cloud services benefit from Availability Zones

Source: https://azure.microsoft.com/en-us/global-infrastructure/geographies/

Paired Regions

- Some regions have designated pair region
- For increased availability
- When a full region fails – the other one can fill its place
- Relevant for some of the cloud services
- Pairs are set by Azure and cannot be changed

Source: https://azure.microsoft.com/en-us/global-infrastructure/geographies/

Azure Services

- Everything that can be done in the cloud is called

Cloud Service

- ie. Creating VMs, building databases, set up networks, use AI algorithms, using central user management etc.

Azure Services

- Go to:

  https://azure.microsoft.com/en-us/services/

Subscription

Logical Container

Contains the various resources you provision in the cloud (VMs, DBs, networks etc.)

Can be attached to a lot of accounts

Account

Identity

An identity with access to resources in the subscription (ie. You)

Can be attached to a lot of subscription

Azure CLI

Run Azure commands from the command line

PowerShell

Run Azure commands from the PowerShell window

- Almost identical capabilities
- Different syntax
- CLI can be run from scripting languages (Python etc.)
- Use whatever you want

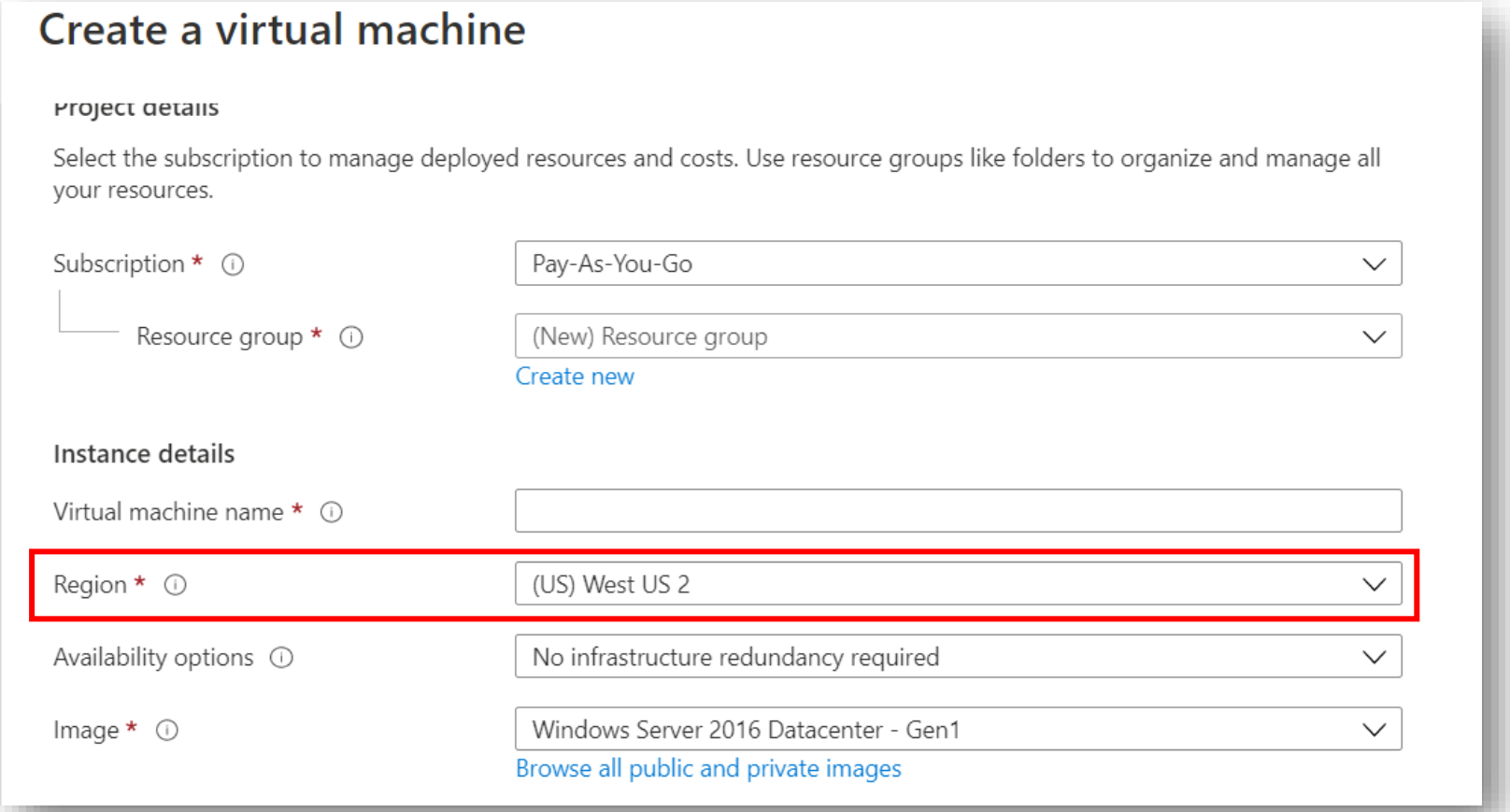
Azure Basic Concepts

Memi Lavi
www.memilavi.com

Source: https://azure.microsoft.com/en-us/global-infrastructure/geographies/

Selecting Regions

- Almost every resource in Azure should be placed in a Region



How to Select Region?

- Geographical proximity to system's audience

How to Select Region?

- Services' availability

TABLE KEY: ✓ Generally Available | ☐ In Preview | ■ In Preview (hover to view expected timeframe) | Future availability (hover to view expected timeframe)

		CANADA		UNITED STATES						
Products	Non-regional	Canada Central	Canada East	Central US	East US	East US 2	North Central US	South Central US	West Central US	West US
Azure Functions		✓	✓	✓	✓	✓	✓	✓	✓	✓
Consumption plan		✓	✓	✓	✓	✓	✓	✓	✓	✓
Consumption plan Linux		Future		✓	✓	✓	✓	✓		✓
Premium plan		✓		✓	✓	✓	✓	✓	✓	✓
Premium plan Linux		✓		✓	✓	✓	✓	✓	✓	✓
Event Grid		✓	✓	✓	✓	✓	✓	✓	✓	✓

Source: https://azure.microsoft.com/en-us/global-infrastructure/services/

How to Select Region?

- Availability Zones

How to Select Region?

- Pricing

REGION: Norway West

OPERATING SYSTEM: Windows

TYPE: (OS Only)

TIER: Standard

INSTANCE: D2 v3: 2 vCPUs, 8 GB RAM, 50 GB Temporary storage, $0.264/hour

VIRTUAL MACHINES: 1 × 730 Hours

Savings Options

Save up to 72% on pay-as-you-go prices with 1-year or 3-year Reserved Virtual Machine Instances. Reserved Instances are great for applications with steady-state usage and applications that require reserved capacity. Learn more about Reserved VM Instances pricing.

Compute (D2 v3)

- (●) Pay as you go
- ( ) 1 year reserved (~36% discount)
- ( ) 3 year reserved (~56% discount)

$125.56
Average per month
($0.00 charged upfront)

OS (Windows)

- (●) License included
- ( ) Azure Hybrid Benefit

$67.16
Average per month
($0.00 charged upfront)

= $192.72
Average per month
($0.00 charged upfront)

How to Select Region?

- Pricing

REGION:
West US

OPERATING SYSTEM:
Windows

TYPE:
(OS Only)

TIER:
Standard

INSTANCE:
D2 v3: 2 vCPUs, 8 GB RAM, 50 GB Temporary storage, $0.209/hour

VIRTUAL MACHINES
1 × 730 Hours

Savings Options

Save up to 72% on pay-as-you-go prices with 1-year or 3-year Reserved Virtual Machine Instances. Reserved Instances are great for applications with steady-state usage and applications that require reserved capacity. Learn more about Reserved VM Instances pricing.

Compute (D2 v3)

- (●) Pay as you go
- ( ) 1 year reserved (~32% discount)
- ( ) 3 year reserved (~57% discount)

$85.41
Average per month
($0.00 charged upfront)

OS (Windows)

- (●) License included
- ( ) Azure Hybrid Benefit

$67.16
Average per month
($0.00 charged upfront)

= $152.57
Average per month
($0.00 charged upfront)

Resource Groups

- A logic container for resources
- Used for grouping resources by a logic boundary
- Free
- Examples:
  - Development / Test / Production resources
  - Team A resources

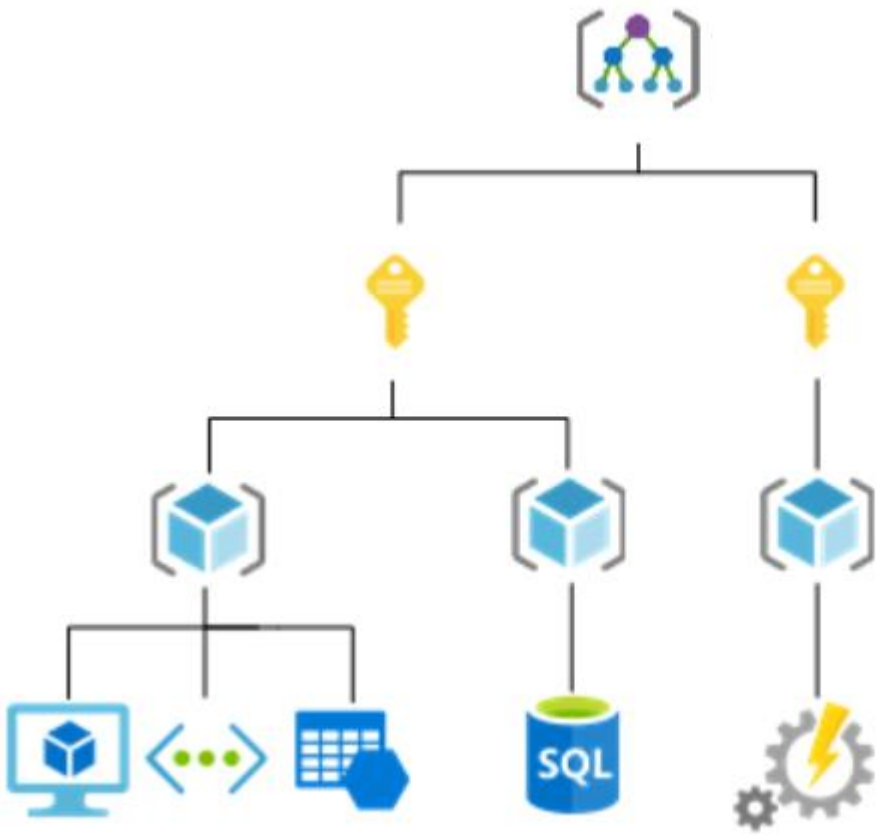
Resource Groups vs Subscriptions

Subscription

Logical Container

Contains the various resources you provision in the cloud (VMs, DBs, networks etc.)

Resource Groups vs Subscriptions



Management groups ← - Manages Subscriptions

Subscriptions ← - Associates accounts
- Cost center

Resource groups ← - Logical Resources Container

Resources

Source: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-setup-guide/organize-resources?tabs=AzureManagementGroupsAndHierarchy

Resource Groups Naming Conventions

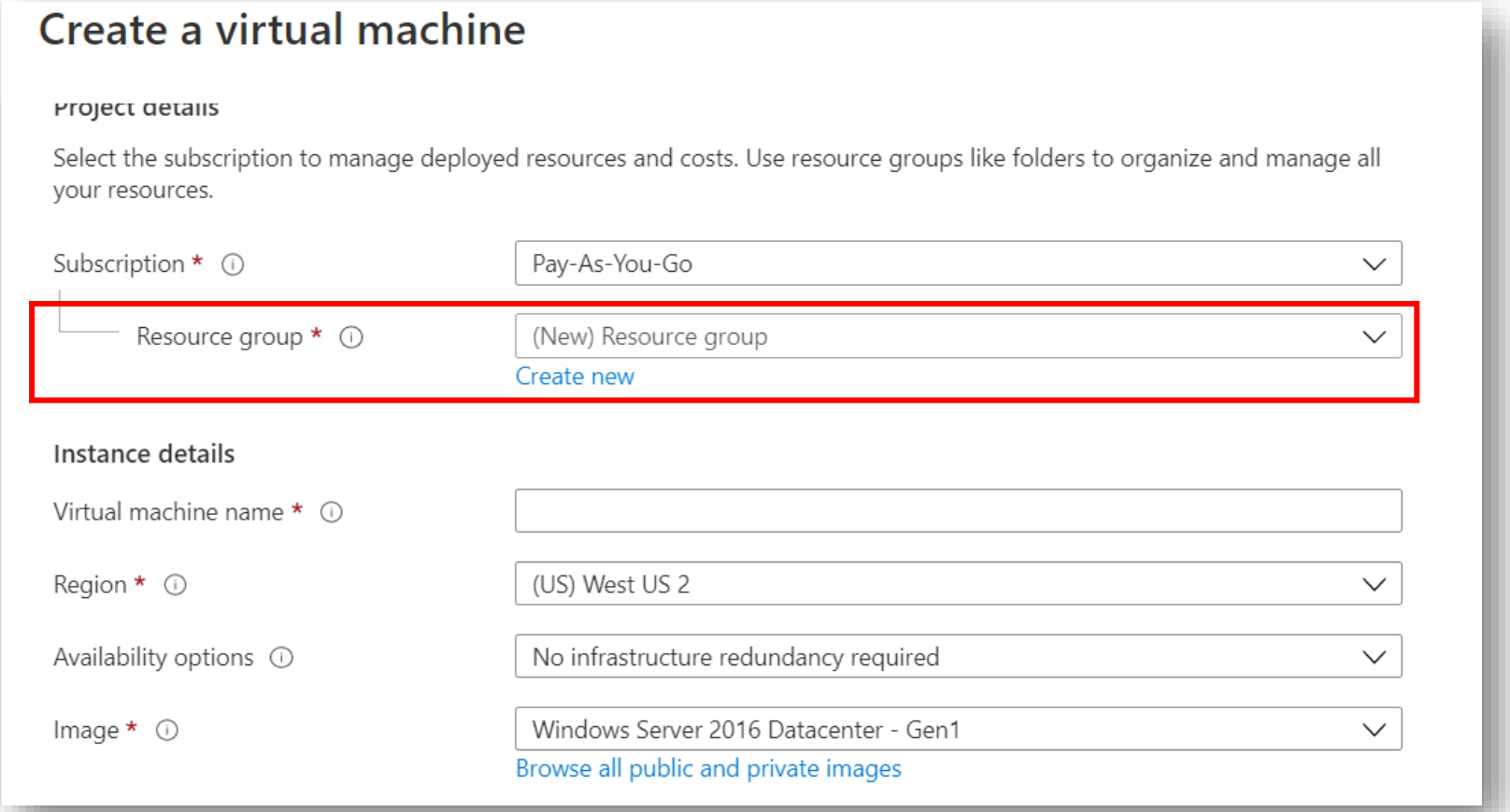
- It's best practice to have an "rg" or "RG" as part of the resource group name
- Could be prefix or suffix

```
RG-Project-Dev

Finance-Resources-rg
```

Resource Groups

- Almost every resource in Azure is placed in a Resource Group



Storage Account

- Used to store almost anything in Azure
- Used transparently by various services
- For example:
  - Database backups
  - VM Disks
  - Diagnostics data

Storage Account

- Used also for explicit data storage
- We'll discuss it later…
- Quite cheap

SLA

- Service Level Agreement
- The uptime % of a cloud service

SLA (%)	Yearly Downtime Allowed
95	18d 6h 17m 27s
99	3d 15h 39m 29s
99.9	8h 45m 56s
99.99	52m 35s

SLA

- ALWAYS check the SLA of the service used

SLA for App Service

Last updated: July 2016

We guarantee that Apps running in a customer subscription will be available 99.95% of the time. No SLA is provided for Apps under either the Free or Shared tiers.

SLA

- ALWAYS check the SLA of the service used

SLA for Azure SQL Database

Last updated: July 2019

Azure SQL Database is a fully managed relational database with built-in regional high availability and turnkey geo-replication to any Azure region. It includes intelligence to support self-driving features such as performance tuning, threat monitoring, and vulnerability assessments and provides fully automated patching and updating of the code base.

- Azure SQL Database Business Critical or Premium tiers configured as Zone Redundant Deployments have an availability guarantee of at least 99.995%.
- Azure SQL Database Business Critical or Premium tiers not configured for Zone Redundant Deployments, General Purpose, Standard, or Basic tiers, or Hyperscale tier with two or more replicas have an availability guarantee of at least 99.99%.
- Azure SQL Database Hyperscale tier with one replica has an availability guarantee of at least 99.95% and 99.9% for zero replicas.

SLA Calculation

- To get the actual system SLA, multiply the SLAs of the participating services

  App Service SLA = 99.95%

  Azure SQL SLA = 99.99%

  Actual SLA = 99.95 X 99.99 = 99.94% = 5h 15m 34s annual downtime

Cost

- Almost everything in the cloud costs money
- Few pricing models:
  - Per resource (ie. VM)
  - Per consumption (ie. Function Apps)
  - Reservations

Cost

- ALWAYS check resource's cost before provisioning
- Check for more cost-effective alternatives
- Look for reservations when available and relevant

Azure Calculator

https://azure.microsoft.com/en-us/pricing/calculator/

Architects and the Cloud

- Software Architects designing regular system need to know:
  - Non-Functional Requirements
  - Technology Stack
  - Component's Architecture
  - Communication Patterns

Architects and the Cloud

- Cloud-based systems require, in addition:
  - Infrastructure knowledge
  - Security
  - Hands-on
- We'll learn all that in this course ☺

Introducing Our App

Memi Lavi
www.memilavi.com

ReadIt!

- Your bookshop on the cloud
- Contains 4 main services:
  - Books catalog
  - Shopping Cart
  - Inventory Management
  - Order Engine

ReadIt!

- Technical details:
  - Developed using .NET Core & nodeJS
    - You don't have to be familiar with these platforms!
  - Uses VS Code
  - Uses various databases

ReadIt!

- What we'll do?
  - Begin with the basic app, run it locally
  - Move it to the cloud, demonstrating various deployment (compute) options
  - Add networking and security
  - Add database support

ReadIt!

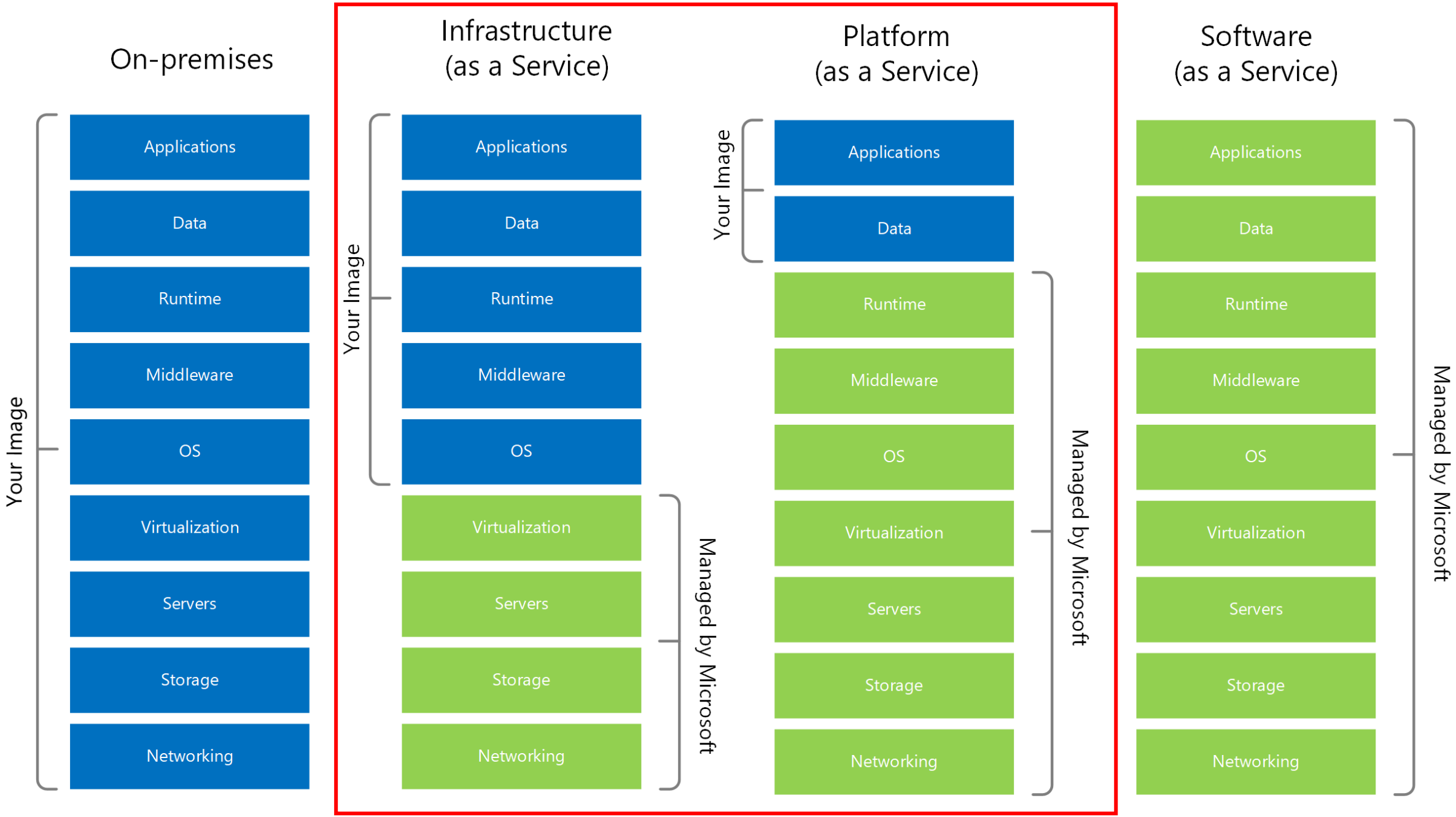
- What we'll do?
  - Add messaging
  - Discuss various alternatives for deployments etc.
  - Keep an eye on the cost…

Azure Compute

Memi Lavi
www.memilavi.com

Compute

- Set of cloud services for hosting and running applications
- Allows uploading your code and then running it
- Offers various levels of control and flexibility



Source: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/strategy/monitoring-strategy

Compute

- We'll talk about 4 types of Compute services:

Virtual Machines

App Services

AKS

Azure Functions

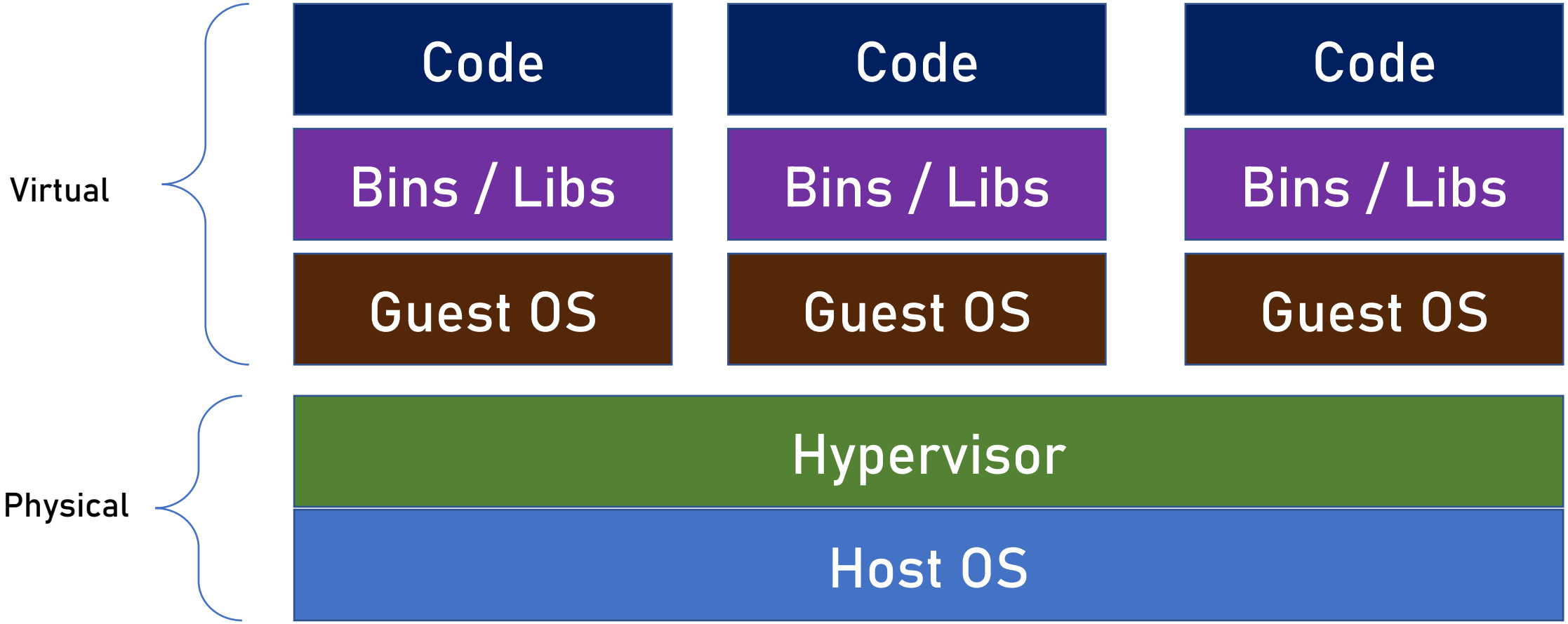
Virtual Machines

- A virtual (=not real) server running on a physical (=real) server
- Allows creating new servers extremely quick
- Based on existing resources of the physical server
- From the user's point of view – a regular server, nothing new
- Called an Unmanaged Service

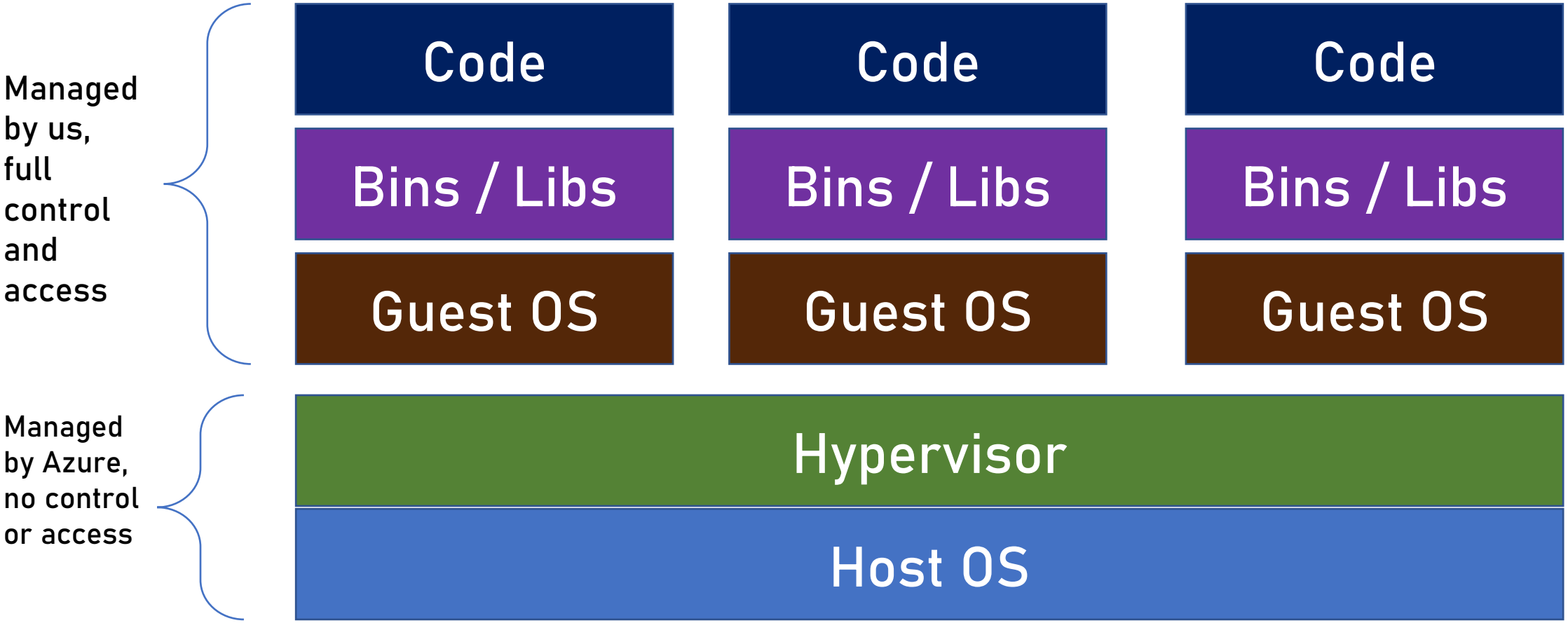
Virtual Machines Architecture

VM Density = No. of VMs per Host

In this case - 3



Virtual Machines In Azure



Virtual Machines in Azure

- Steps for creating VM in Azure:
  - Select the location
  - Select the image (OS or Pre-installed software)
  - Select the size
  - That's it, basically….

Don't forget to check the price!

The Real Cost of VM

- Cost of VM includes:
  - VM
  - Disk
  - IP
  - Storage

The Real Cost of VM

Resource	Type	Monthly Cost ($)
VM	D2v3	154.76
Disk	P10	21.68
Public IP	Dynamic	2.92
Storage	LRS	<1$

Total: ~180$

Reducing the Cost of VM

- Most effective techniques to reduce costs of VM:

Auto Shutdown

Reserved Instances

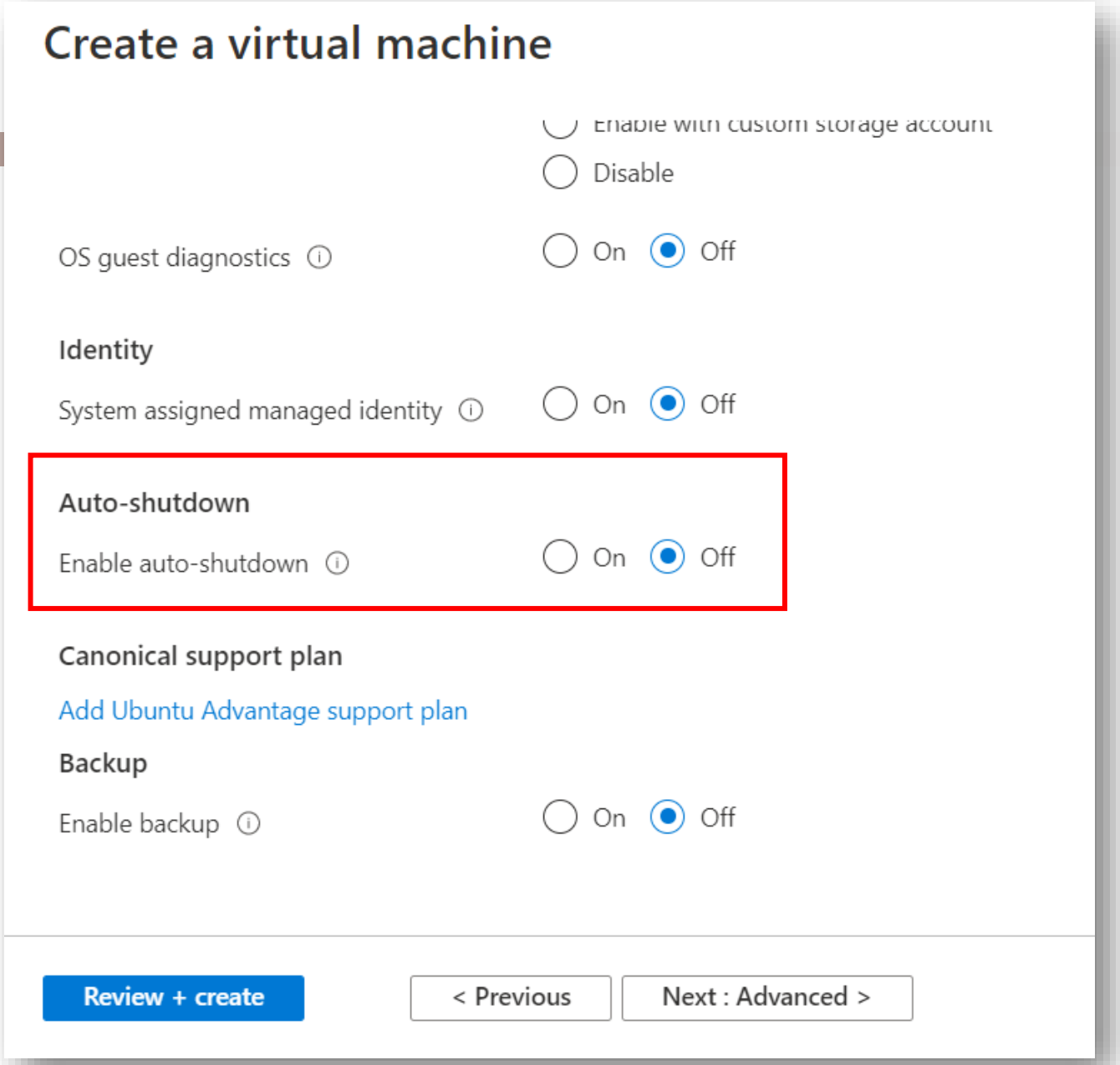
Spot Instances

Disk Optimization

Auto Shutdown

- As simple as it sounds…
- Automatically shuts down the machine when not needed
  - Relevant mainly for test / dev machines
- Storage and IP (if static) costs still incurred
- Can save >50% of VM cost

Auto Shutdown



Reserved Instances

- Allow upfront payment with substantial discount
- Usually offered for 1 or 3 years
  - Great for production machine which run continuously
- Offers great discounts (up to 62%)
- Can be divided to monthly payments
- Cannot be stopped / refunded
  - Unless…

Reserved Instances

Virtual Machines

REGION: West Europe

OPERATING SYSTEM: Linux

TYPE: Ubuntu

TIER: Standard

INSTANCE: D4s v3: 4 vCPUs, 16 GB RAM, 32 GB Temporary storage, $0.24/hour

VIRTUAL MACHINES: 1 × 730 Hours

Savings Options

Save up to 72% on pay-as-you-go prices with 1-year or 3-year Reserved Virtual Machine Instances. Reserved Instances are great for applications with steady-state usage and applications that require reserved capacity. Learn more about Reserved VM Instances pricing.

Compute (D4s v3)

- (●) Pay as you go
- ( ) 1 year reserved (~36% discount)
- ( ) 3 year reserved (~56% discount)

$175.20
Average per month
($0.00 charged upfront)

= $175.20
Average per month
($0.00 charged upfront)

Spot Instances

- Machines that run on unused capacity in Azure
- Can be evicted any moment when needed by Azure
- Offers up to 90% discount, price fluctuates according to demand
- Great for non-critical, non-continuous tasks
  - ie. Batch processes, long running calculations

Spot Instances

Create a virtual machine

Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.

Availability options: No infrastructure redundancy required

Image *: Ubuntu Server 18.04 LTS - Gen1

Browse all public and private images

Azure Spot instance: (•) Yes ( ) No

Eviction type:
(•) Capacity only: evict virtual machine when Azure needs the capacity for pay as you go workloads. Your max price is set to the pay as you go rate.
( ) Price or capacity: choose a max price and Azure will evict your virtual machine when the cost of the instance is greater than your max price or when Azure needs the capacity for pay as you go workloads.

Eviction policy: (•) Stop / Deallocate ( ) Delete

Size *: Standard_D2s_v3 - 2 vcpus, 8 GiB memory ($0.02005/hour)

Select size

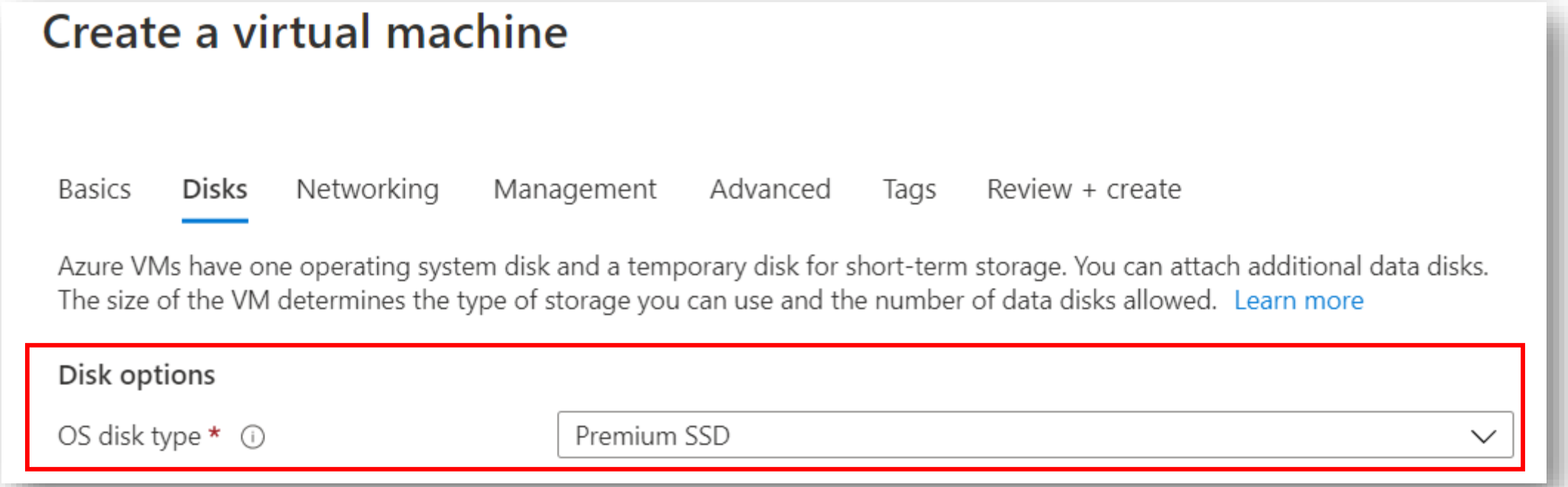
View pricing history and compare prices in nearby regions

Review + create | < Previous | Next : Disks >

Disk Optimization

- Make sure to select the right disk for the machine
- Default is Premium SSD – the most expensive option
- Non IO-intensive machines can do with Standard SSD
  - ie. App servers, in-memory cache
- Note: Disk type affects the SLA

Disk Optimization



More Cost Saving Techniques

- Select the right size for your machine
  - CPU shouldn't rest, you pay for it☺
- Select Linux over Windows when possible
- Check price in nearby regions

Availability of a VM

SLA (%)	Yearly Downtime Allowed
95	18d 6h 17m 27s
99.5	1d 19h 49m 44s
99.9	8h 45m 56s
99.95	4h 22m 44s
99.99	52m 35s

SLA for Virtual Machines

Last updated: July 2020

- For all Virtual Machines that have two or more instances deployed across two or more Availability Zones in the same Azure region, we guarantee you will have Virtual Machine Connectivity to at least one instance at least 99.99% of the time.
- For all Virtual Machines that have two or more instances deployed in the same Availability Set or in the same Dedicated Host Group, we guarantee you will have Virtual Machine Connectivity to at least one instance at least 99.95% of the time.
- For any Single Instance Virtual Machine using Premium SSD or Ultra Disk for all Operating System Disks and Data Disks, we guarantee you will have Virtual Machine Connectivity of at least 99.9%.
- For any Single Instance Virtual Machine using Standard SSD Managed Disks for Operating System Disk and Data Disks, we guarantee you will have Virtual Machine Connectivity of at least 99.5%.
- For any Single Instance Virtual Machine using Standard HDD Managed Disks for Operating System Disks and Data Disks, we guarantee you will have Virtual Machine Connectivity of at least 95%.

Source: https://azure.microsoft.com/en-us/support/legal/sla/virtual-machines/v1_9/

Availability Concepts in Azure

Fault Domain

Update Domain

Availability Set

Availability Zone

Fault Domain

- Logical group of physical hardware that share a common power source and network switch
- Similar to rack in a traditional data center

Fault Domain

If there's a problem with the power or networking in the domain (=rack) – all servers in it shut down

↓

You want to make sure your servers are spread across more than one fault domain (=rack)

Update Domain

- Logical group of physical hardware that can undergo maintenance and be rebooted at the same time
- Maintenance is done by Azure at its own discretion

Update Domain

If all your servers are in the same update domain –

they'll reboot at the same time during maintenance

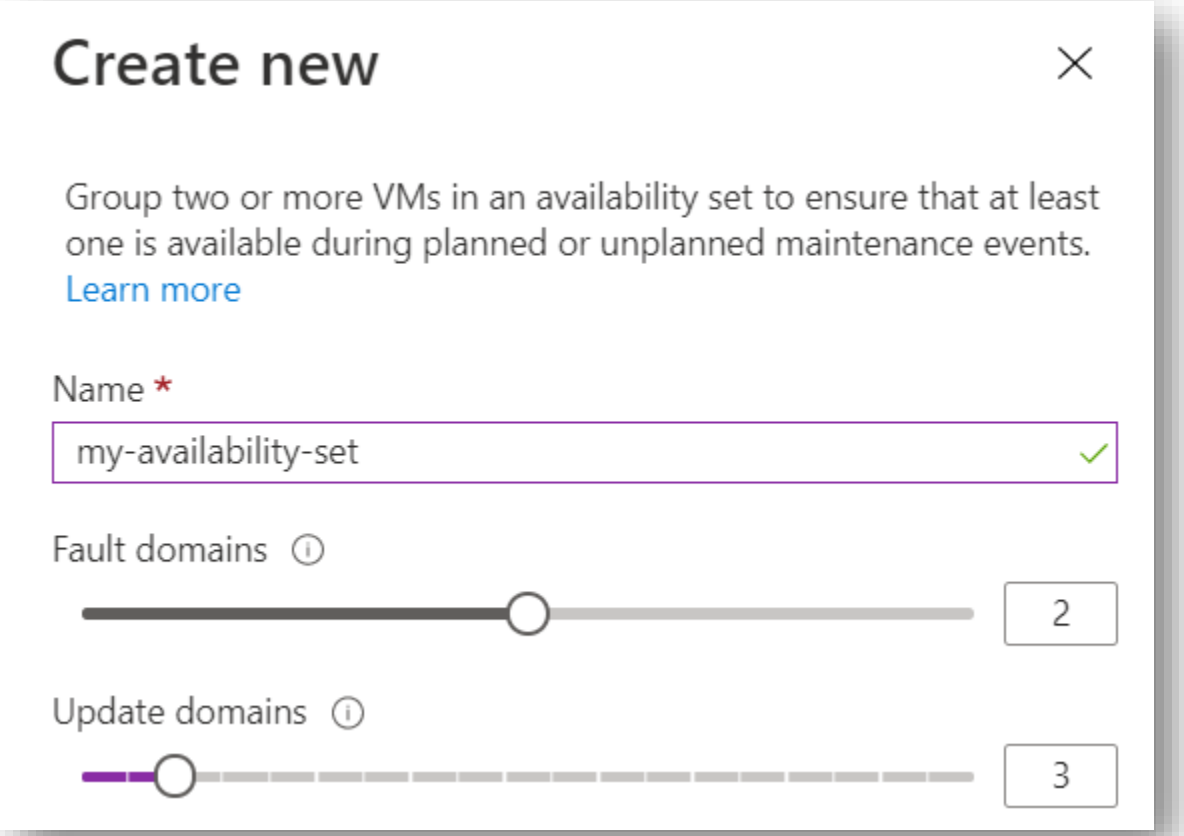
You want to make sure your servers are spread

across more than one update domain

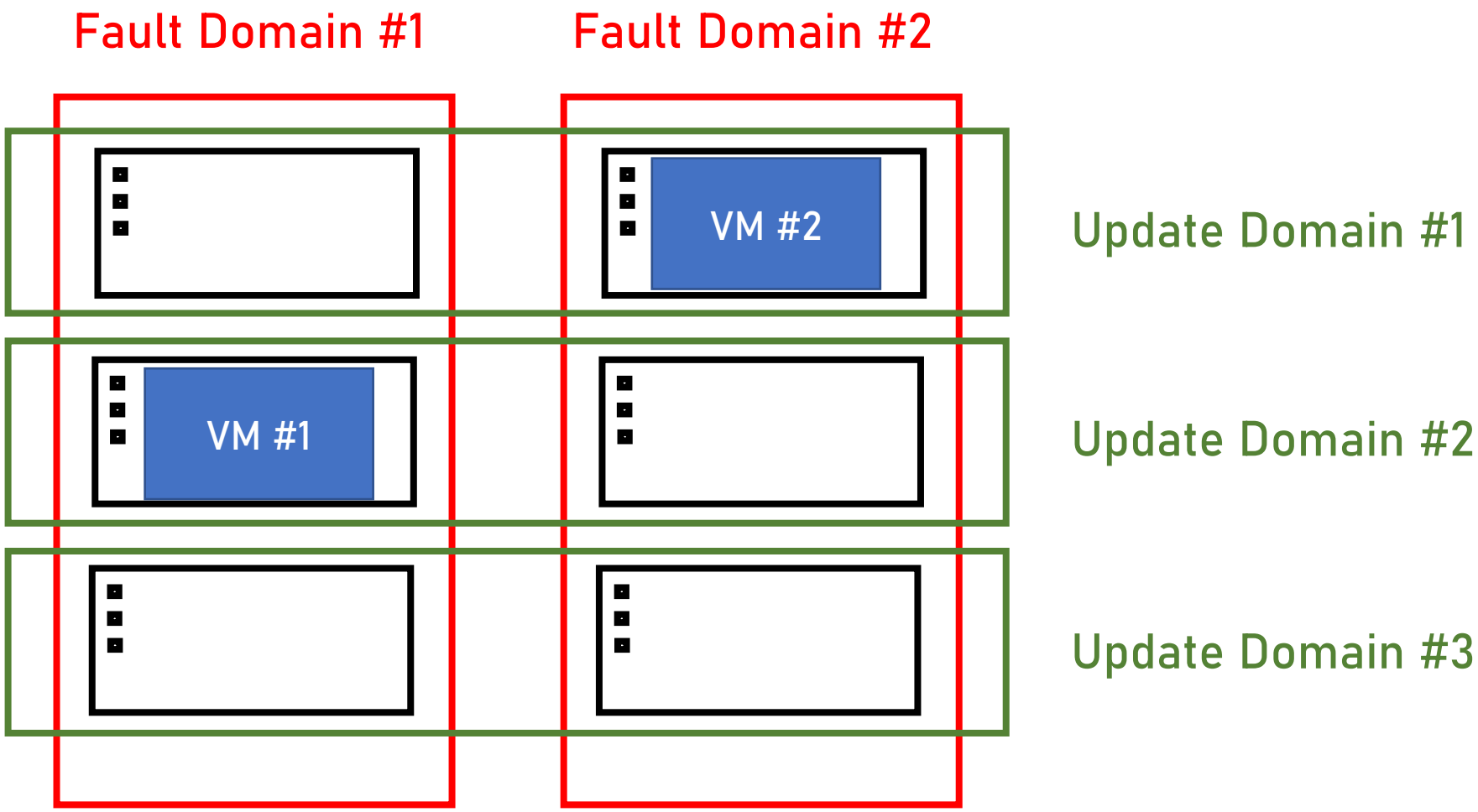
Availability Set

- A collection of Fault Domains and Update Domains your VMs will be spread across
- Can contain up to 3 Fault Domains and up to 20 Update Domains
- All domains (Fault & Update) are in the same Zone (=datacenter)

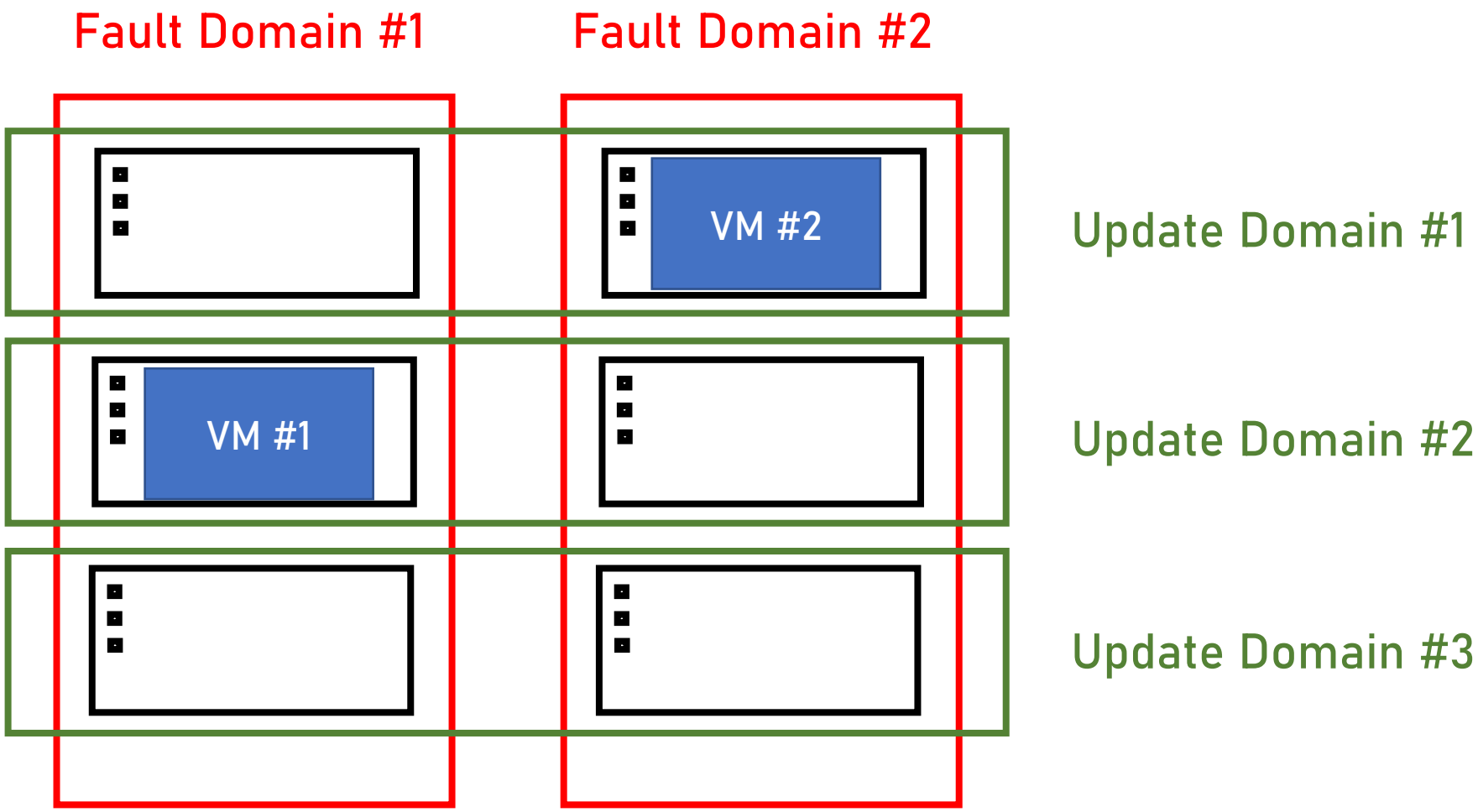
Availability Set Example



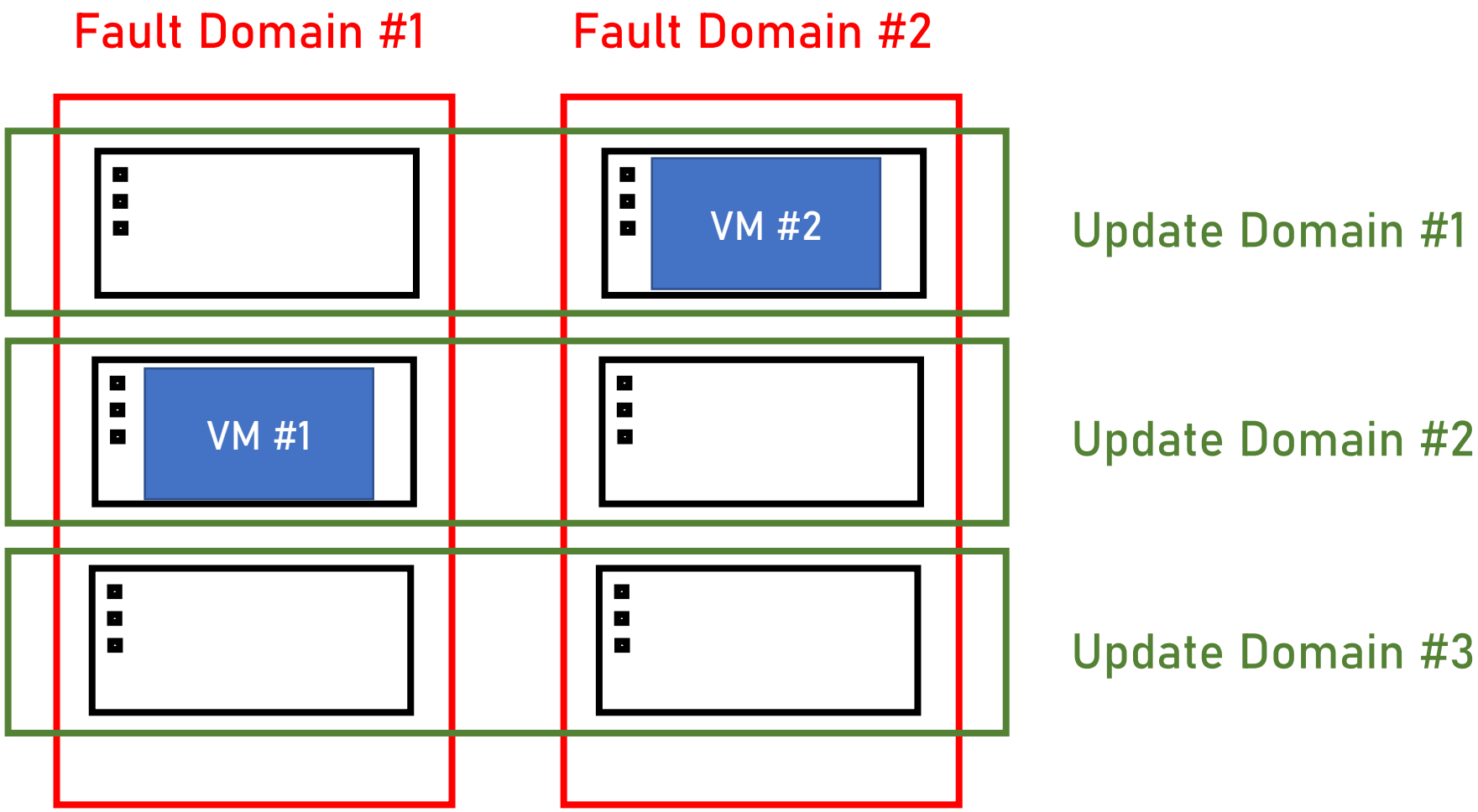
Availability Set Example



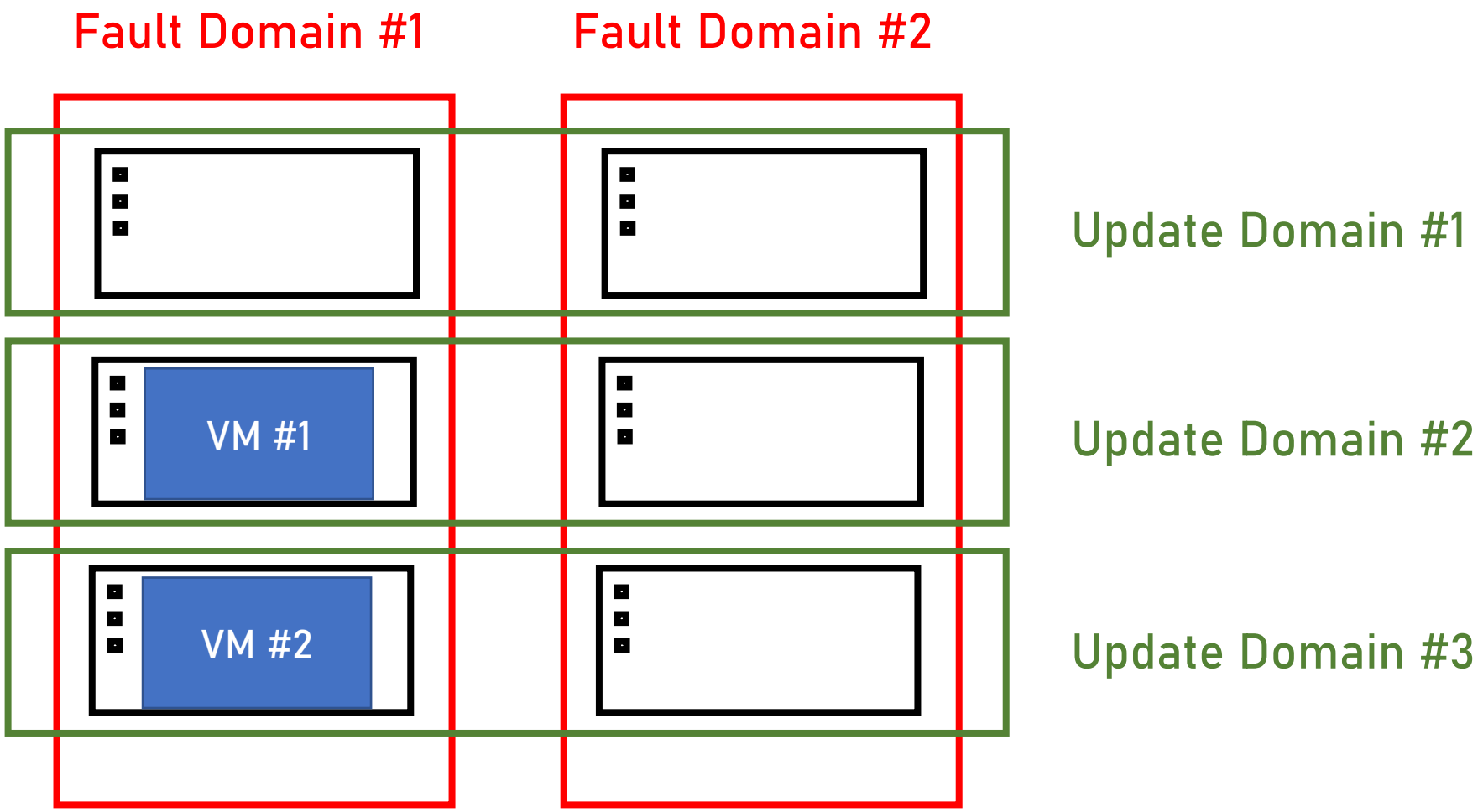
Update Domain #2 Reboots



Fault Domain #1 Fails



Without Availability Set…



Taking Advantage of Availability Set

- Deploy identical VMs into the same Availability Set
- Ensures they won't be shut down simultaneously when a single fault domain shuts down or an update domain reboots
- If needed – deploy load balancer to route between the VMs
- Availability Set is free, you pay only for the additional VMs

Availability Zone

- A physically separate zone within an Azure region
- Technically – a building containing an autonomous data center
- Each zone functions as a fault & update domain
- Provides protection against a complete zone shutdown
  - Hence the better SLA

Taking Advantage of Availability Zone

- Deploy identical VMs into separate Availability Zones in the same Region
- Ensures they won't be shut down simultaneously when the zone shuts down
- If needed – deploy load balancer to route between the VMs
- Availability Zone is free, you pay only for the additional VMs

ARM Template

- Azure Resource Manager Template
- A JSON file describing the resource(s) to be created
- Used by Azure in (almost) all deployments
- Can be exported, modified, uploaded, deployed
- Can also be created from scratch

ARM Template

- ARM Template is a declarative way of deploying resources

Declarative

- Describes the end result
- Allows “What-If” operation
- Can deploy multiple resources at once
- Can be integrated in CI/CD processes
- Can be source controlled

Used by: ARM Template

Imperative

- Sends instructions to run
- Error prone
- Can’t be verified
- Can’t be source controlled
- Suited for quick and dirty operations

Used by: Azure CLI, PowerShell

(Although they can run ARM Template too)

Virtual Machine Scale Set

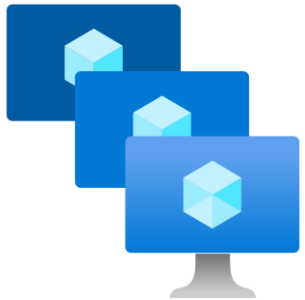
- A group of separate VMs sharing the same image
- Managed as a group
- Can be scaled out or in manually or according to predefined conditions
- Great for handling unpredictable load

Virtual Machine Scale Set

- Once set up, the machines should NOT be modified
  - Change files, install apps etc.
- New machines created by the scale set will be based on the original image
- For web apps, a load balancer should be put in front of the scale set

Scale Set Architecture

Load Balancer



Virtual Machine Scale Set
(VMSS)

Scale Set Pricing

- Scale Set is free
- You pay for the VMs deployed in it

Azure Instance Metadata Services

- A little known feature of Azure VMs
- A REST API accessible from the VM
- Providing a lot of info about the machine
- Info includes:
  - SKU, storage, networking, scheduled events
- Accessible ONLY from the VM

Azure Instance Metadata Services

- With Scaleset –
  - Get notification about upcoming eviction
- Can be polled every ~1 min to get enough time to close things up

Azure Architecture Diagram

- When designing architecture for Azure apps it's a good idea to use Azure symbols in the diagram
- There are hundreds of them…

Download Azure Icons

- https://docs.microsoft.com/en-us/azure/architecture/icons/

ReadIt!

Cloud Architecture

VM
Weather API

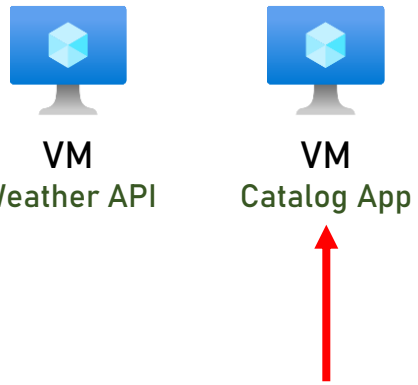
VM
Catalog App

Cloud Architecture

A Word of Caution:

NEVER
leave a VM open to the internet this way

We will learn later on what should be done



- Directly accessible from the internet
- Can be RDPed from anywhere

App Services

- A fully managed web hosting for websites
- Publish your code – and it just runs
- No access to the underlying servers
- Secured and compliant
- Integrates with many source controls and DevOps engines:
  - GitHub, BitBucket, Azure DevOps, DockerHub and more

App Services

- Supported platforms:
  - .NET
  - .NET Core
  - Node.JS
  - Java
  - Python
  - PHP
- Supports containers

App Services

- App Types:
  - Web Apps
  - Web API
  - Web Jobs (batch processes)

App Services

- Extremely easy to deploy:

    1. Develop your app
    2. Create Web App (can be done from the IDE)
    3. Publish your code
    4. Viola!

App Services Tiers

OS/Software: Linux | Region: West Europe | Currency: US Dollar ($) | Display pricing by: Month

	FREE Try for free	BASIC Dedicated environment for dev/test	STANDARD Run production workloads	PREMIUM Enhanced performance and scale	ISOLATED High-Performance, Security and Isolation
Web, mobile, or API apps	10	Unlimited	Unlimited	Unlimited	Unlimited
Disk space	1 GB	10 GB	50 GB	250 GB	1 TB
Maximum instances	–	Up to 3	Up to 10	Up to 30*	Up to 100
Custom domain	–	Supported	Supported	Supported	Supported
Auto Scale	–	–	Supported	Supported	Supported
Hybrid Connectivity	–	Supported	Supported	Supported	Supported
Virtual Network Connectivity	–	–	Supported	Supported	Supported
Private Endpoints	–	–	–	Supported	Supported
Compute Type	Shared	Dedicated	Dedicated	Dedicated	Isolated
Pay as you go price	Free	Promotional Price ~$13.140/month	~$69.35/month	~$83.95/month	~$208.050/month

Lowest price, goes up with CPU & RAM

Source: https://azure.microsoft.com/en-us/pricing/details/app-service/linux/

App Service Auto Scaling

- App Service can be autoscaled to support spikes in load
- Auto scale is based on various metrics
- Extremely flexible

App Service Auto Scaling

Default* Auto created scale condition

Delete warning

The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.

Scale mode

Scale based on a metric | Scale to a specific instance count

Rules

It is recommended to have at least one scale in rule. New rules can be created by click hyperlink Add a rule .

Scale out

When	Default1	(Average) CpuPercentage > 70	Increase count by 1
Or	Default1	(Average) HttpQueueLength > ...	Increase count by 1

+ Add a rule

Instance limits

Minimum	Maximum	Default
1	3	1

Schedule

This scale condition is executed when none of the other scale condition(s) match

Deployment Slots

- When uploading code to App Service the new version is accessible immediately
- Sometimes we want to test the version before publishing it
- Deployment Slots allow us to upload code and test it separately from the main site
- After validation we swap the slots and promote it to production

Deployment Slots

- New slots are created from the portal
- Number of allowed slots depends on plan
  - ie. Standard plans allow for up to 5 slots
- Slot is a fully functional app service with a dedicated URL
- Slots can be accessed directly through their URL
- Free

Deployment Slots Traffic Splitting

- Traffic can be split between slots
- Some users will be routed to the production and some to the new slot
- Great for some deployment scenarios

Deployment Types

- Traffic Splitting enables various types of deployment

Basic

Rolling

Blue-Green

Basic Deployment

- All instances update to the new version at once

v1

v2

Basic Deployment

- All instances update to the new version at once

v1

v2

Basic Deployment

Pros

- Simple
- Fast

Cons

- Risky
- System might get unusable

Basic Deployment

- App Service implementation:
  - Simple deployment of new version
  - No use of deployment slots

Rolling Deployment

- Instances are updated gradually in batches
- Only if no errors are found the deployment resumes

v1

v2

Rolling Deployment

- Instances are updated gradually in batches
- Only if no errors are found the deployment resumes

v1

v2

Rolling Deployment

- Instances are updated gradually in batches
- Only if no errors are found the deployment resumes

v1

v2

Rolling Deployment

- Instances are updated gradually in batches
- Only if no errors are found the deployment resumes

v1

v2

Rolling Deployment

Pros

- Allows rollback

Cons

- Need to support two versions simultaneously
- Not easy to manage

Rolling Deployment

- App Service implementation:
  - Deploy to slot
  - Set traffic percentage so that small % will be routed to the new version
  - Gradually increase % of traffic to new version until 100%
  - Swap slots

Blue-Green Deployment

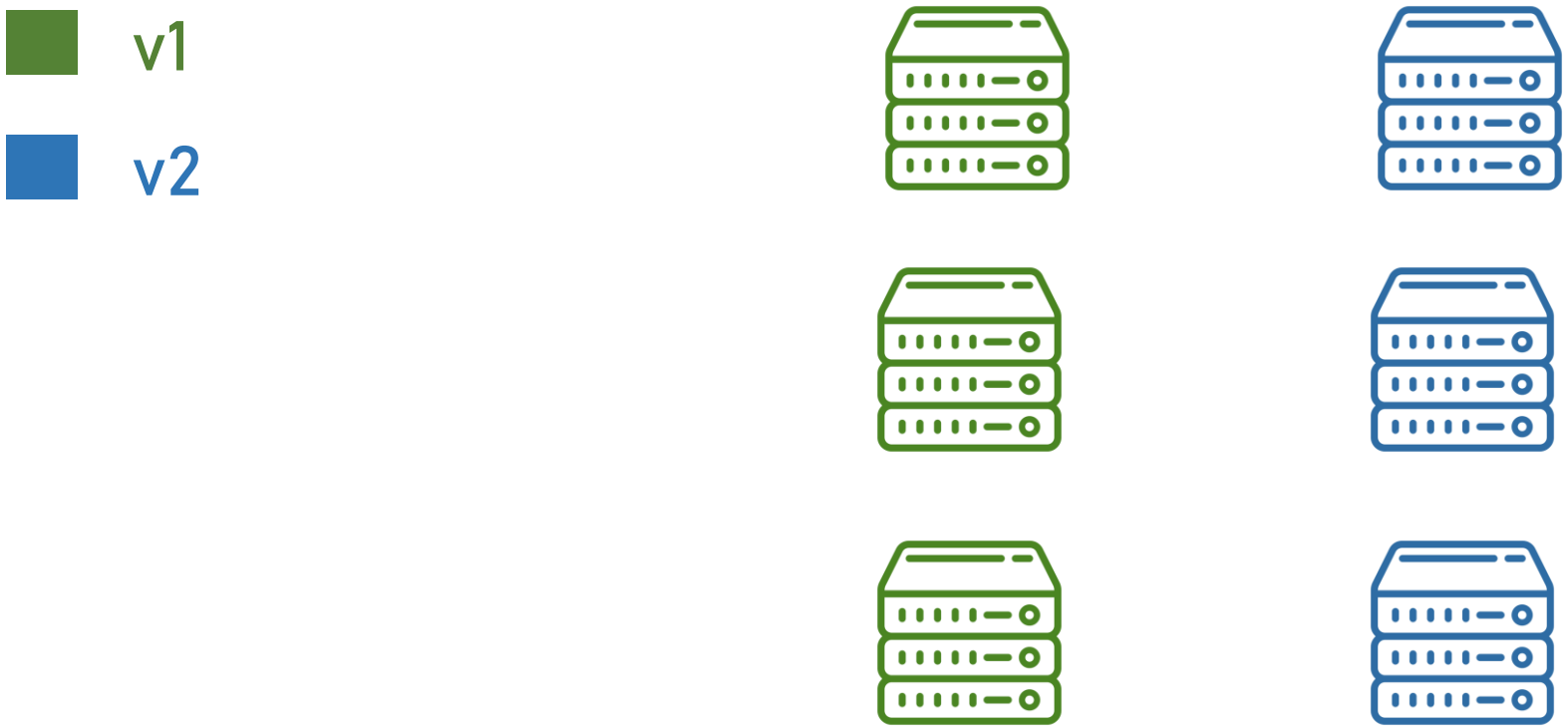
- New version uploaded and accessible only to testers
- After verification complete, traffic is routed to new version

v1

v2

Blue-Green Deployment

- New version uploaded and accessible only to testers
- After verification complete, traffic is routed to new version



Blue-Green Deployment

- New version uploaded and accessible only to testers
- After verification complete, traffic is routed to new version

v1

v2

Blue-Green Deployment

Pros

- Simple
- New environment is always tested

Cons

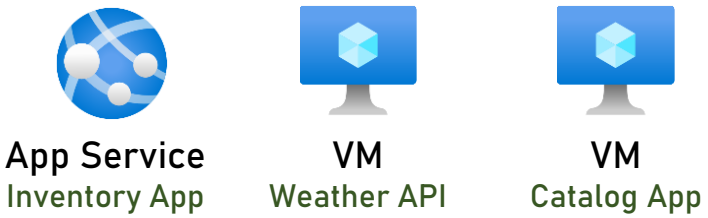
- Cost
  - More instances

Blue-Green Deployment

- App Service implementation:
  - Deploy to a new slot
  - Testers work on the new slot using its dedicated URL
  - After testing is complete – swap slots

ReadIt!

Cloud Architecture

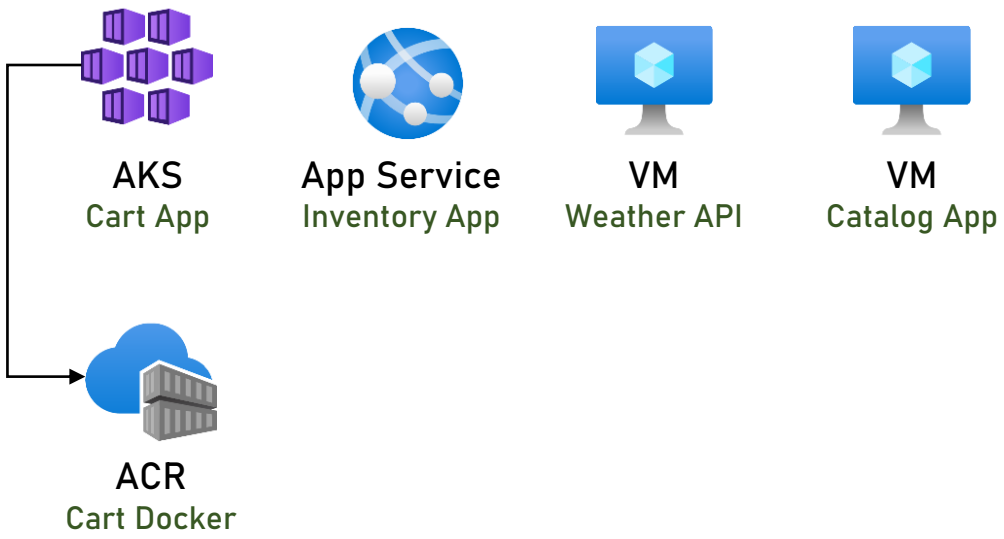


AKS

- Azure Kubernetes Services
- Managed Kubernetes on Azure
- Allows deploying containers and managing them using Kubernetes on Azure
- Paying only on the instances (=VMs) used

ReadIt!

Cloud Architecture



Azure Functions

- Small, focused functions running as a result of an event
- Great for Event Driven systems
- Automatically managed by Azure
  - Start, stop, autoscale
- Flexible pricing plans
- Serverless

Serverless

- Cloud resource that is completely managed by the cloud
- Users do not need to think about:
  - VMs
  - CPU
  - Memory
  - etc.
- It just works

Serverless

Remember:

Azure Function Example

```
namespace AzureCourse.Function
{
    0 references
    public static class EventGridFunction
    {
        [FunctionName("EventGridFunction")]
        0 references
        public static async Task Run(
            [HttpTrigger(AuthorizationLevel.Anonymous, "get", "post", Route = null)] HttpRequest req,
            [EventGrid(TopicEndpointUri = "MyEventGridTopicUriSetting", TopicKeySetting = "MyEventGridTopicKeySetting")]
                IAsyncCollector<EventGridEvent> outputEvents,
            ILogger log)
        {
            string name = req.Query["name"];

            var myEvent = new EventGridEvent("message-id-3", "user-added", $"{{name: {name} }}", "event-type", DateTime.UtcNow, "1.0");
            await outputEvents.AddAsync(myEvent);

        }
    }
}
```

Triggers and Bindings

Triggers

- The event that made the function run
- Quite a few
- Deeply integrated into other Azure services
- Technically not mandatory, but…

Bindings

- Declarative connection to other resource(s)
- Input, output, or both
- Provided as parameter to the function
- Makes connecting to other resources extremely easy
- Not mandatory

Azure Function Example

```
namespace AzureCourse.Function
{
    0 references
    public static class EventGridFunction
    {
        ventGridFunction")]

        public static async Task Run(
            [HttpTrigger(AuthorizationLevel.Anonymous, "get", "post", Route = null)] HttpRequest req,
            [EventGrid(TopicEndpointUri = "MyEventGridTopicUriSetting", TopicKeySetting = "MyEventGridTopicKeySetting")]
                IAsyncCollector<EventGridEvent> outputEvents,
            ILogger log)

            Query["name"];

            var myEvent = new EventGridEvent("message-id-3", "user-added", $"{{name: {name} }}", "event-type", DateTime.UtcNow, "1.0");
            await outputEvents.AddAsync(myEvent);

        }
    }
}
```

Trigger (HTTP)

Binding (EventGrid)

Trigger Types

- Blob Storage
- Cosmos DB
- Dapr
- Event Grid
- Event Hubs
- HTTP Requests
- IOT Hub
- Kafka
- Queue Storage
- RabbitMQ
- Service Bus
- Timer

Binding Types (Input or Output)

- Blob Storage
- Cosmos DB
- Dapr
- Event Grid
- Event Hubs
- HTTP Requests
- IOT Hub
- Kafka
- Mobile Apps
- Notification Hub
- Queue Storage
- RabbitMQ
- SendGrid
- Service Bus
- SignalR
- Table Storage

Triggers and Bindings

- Example scenarios:
  - Run every 5 minutes (*Timer Trigger)* and calculate the sum of a column in a DB. If it's above 115, send an event in EventGrid (*Binding)*

Triggers and Bindings

- Example scenarios:
  - When a message arrives in the Orders Queue (*Queue Trigger)*

    save it in Cosmos DB (*Binding)* for future handling

Triggers and Bindings

- Example scenarios:
  - Receive HTTP Request (*HTTP Trigger)* with 4 numbers, and return the smallest one of them (*no binding)*

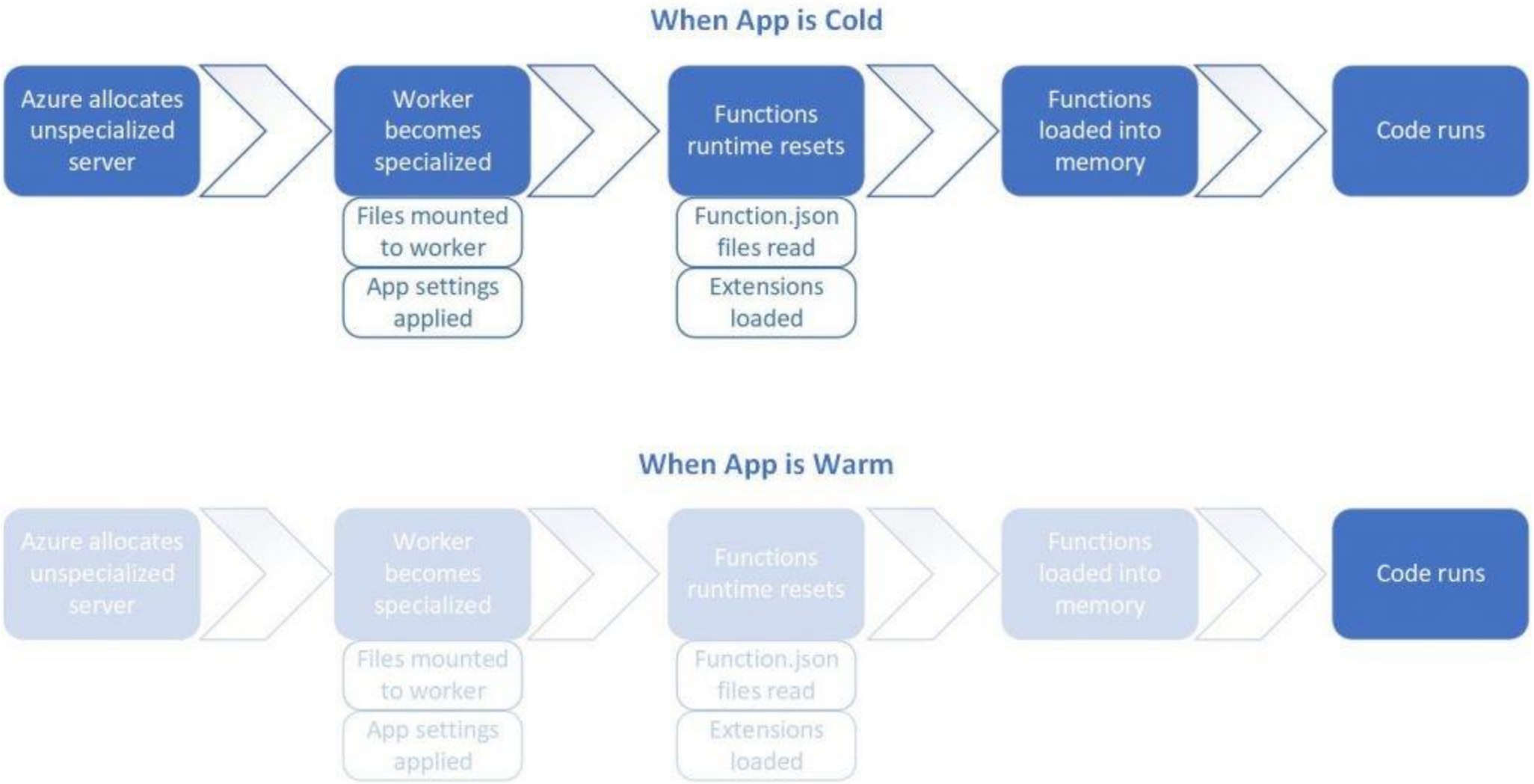
Supported Languages

- C#
- JavaScript (nodeJS)
- Java
- Python
- PowerShell
- F#

Cold Start

- Azure Functions are completely managed by Azure
- After some time of inactivity Azure might take down the Function's host
- The next activation of the Function will take time
  - 2-3 seconds before the code runs
- A problem mainly for HTTP-Triggered functions

Cold Start



Source: https://azure.microsoft.com/en-us/blog/understanding-serverless-cold-start/

Cold Start

- How to avoid cold start?
  - Select the right hosting plan

Azure Functions Hosting Plans

Consumption

Premium

Dedicated

Consumption Plan

- Pay only for what you actually use

METER	PRICE	FREE GRANT (PER MONTH)
Execution Time*	$0.000016/GB-s	400,000 GB-s
Total Executions*	$0.20 per million executions	1 million executions

*Free grants apply to paid, consumption subscriptions only.

Note—A storage account is created by default with each Functions app. The storage account is not included in the free grant. Standard storage rates and networking rates charged separately as applicable.

- Note: In consumption plan there's a limit of 1.5GB RAM

Consumption Plan

- Calculation example:

METER	PRICE	FREE GRANT (PER MONTH)
Execution Time*	$0.000016/GB-s	400,000 GB-s
Total Executions*	$0.20 per million executions	1 million executions

- Executions / month: 9m
- Avg. memory consumed / execution: 800MB
- Avg. execution duration: 1.5s

- Total seconds: 9m * 1.5s = 13.5m secs
- Total GB / sec = 13.5m * 0.8 = 10.8m – 400K free grant = 10.4m GB/sec
- Payment for execution time: 10.4m * 0.000016$ = 166.4$
- Payment for executions: 9m-1m free grant = 8m * 0.2$ / m = 1.6$

Total Payment: 168$

Consumption Plan

- Downsides:
  - 1.5GB RAM limit
  - Cold Start

Premium Plan

- Pay for pre-warmed instances (hosts)

METER	PRICE
vCPU duration	vCPU: ~$123.37 vCPU/month
Memory duration	Memory: ~$8.833 GB/month

INSTANCE:

EP1: 1 Cores(s), 3.5 GB RAM, 250 GB Storage

EP1: 1 Cores(s), 3.5 GB RAM, 250 GB Storage

EP2: 2 Cores(s), 7 GB RAM, 250 GB Storage

EP3: 4 Cores(s), 14 GB RAM, 250 GB Storage

Instances

- Pay for scale-out instances

Premium Plan

- What you get:
  - No cold starts
  - No memory limit (up to host RAM)
  - Better performance
  - VNet integration
  - Predictable price

Premium Plan

- Calculation example:

METER	PRICE
vCPU duration	vCPU: ~$123.37 vCPU/month
Memory duration	Memory: ~$8.833 GB/month

- 1 pre-warmed instance
- 2 vCpus, 7GB RAM
- No scale out

- vCPU cost: 123.37 X 2 = 246.74$
- Memory cost: 8.833 X 7 = 61.83$

Total Payment: 308.57$

Premium Plan

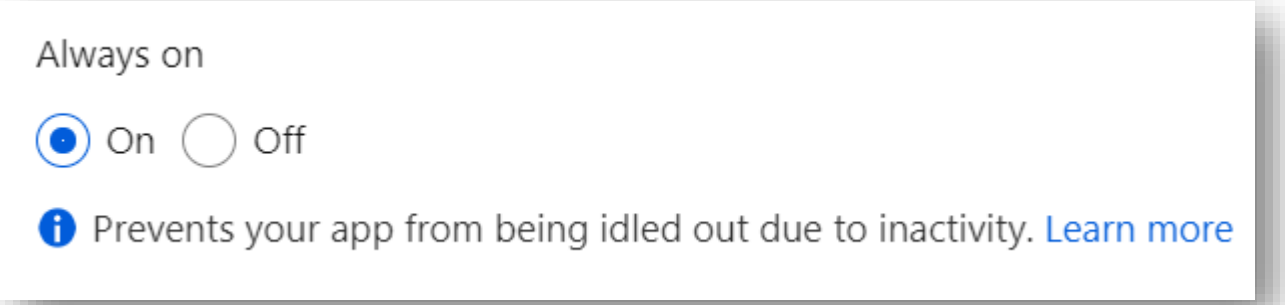
- Downsides:
  - More expensive

Dedicated Plan

- The Functions run on an existing App Service
- Great if server is under-utilized
- No additional costs

Dedicated Plan

- Make sure Always On setting is activated to avoid disabling functions:



Dedicated Plan

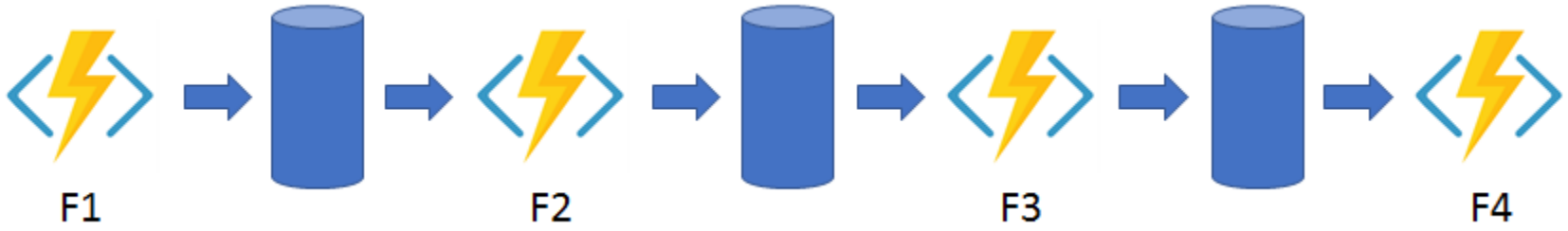
- Downsides:
  - No Auto-Scale

Durable Functions

- Stateful Functions that interact with external resources and keep track of flow
- Offer very simple syntax, hide complexities of managing state, retries, etc.

Durable Functions

- For example:
  - Function Chaining – call various Functions sequentially, and apply the output of each function to the next one:

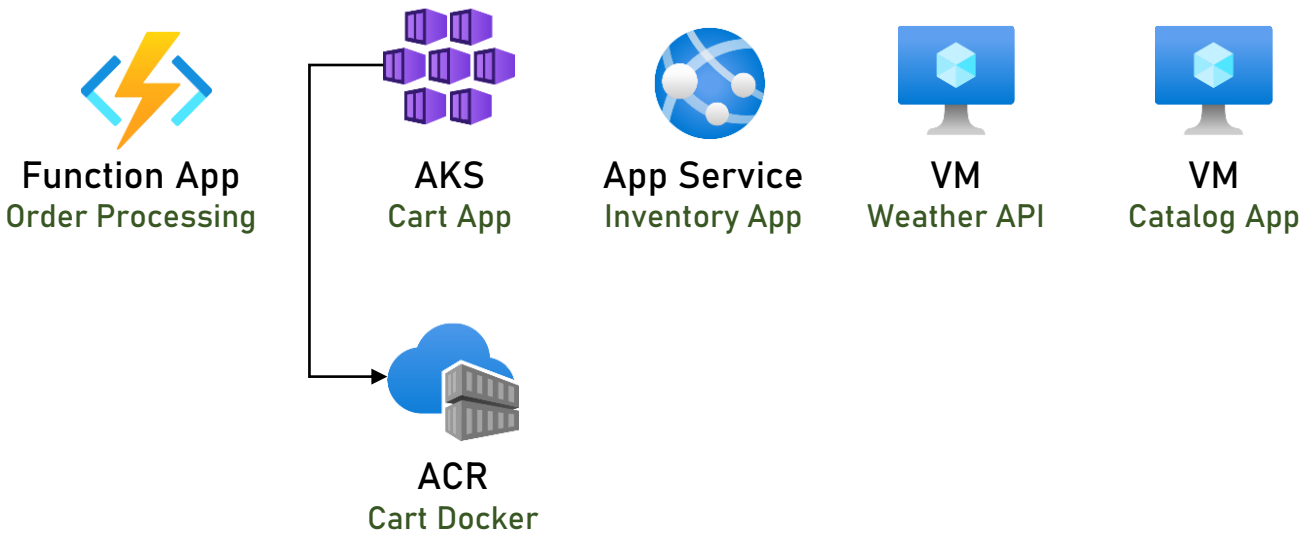


Durable Functions

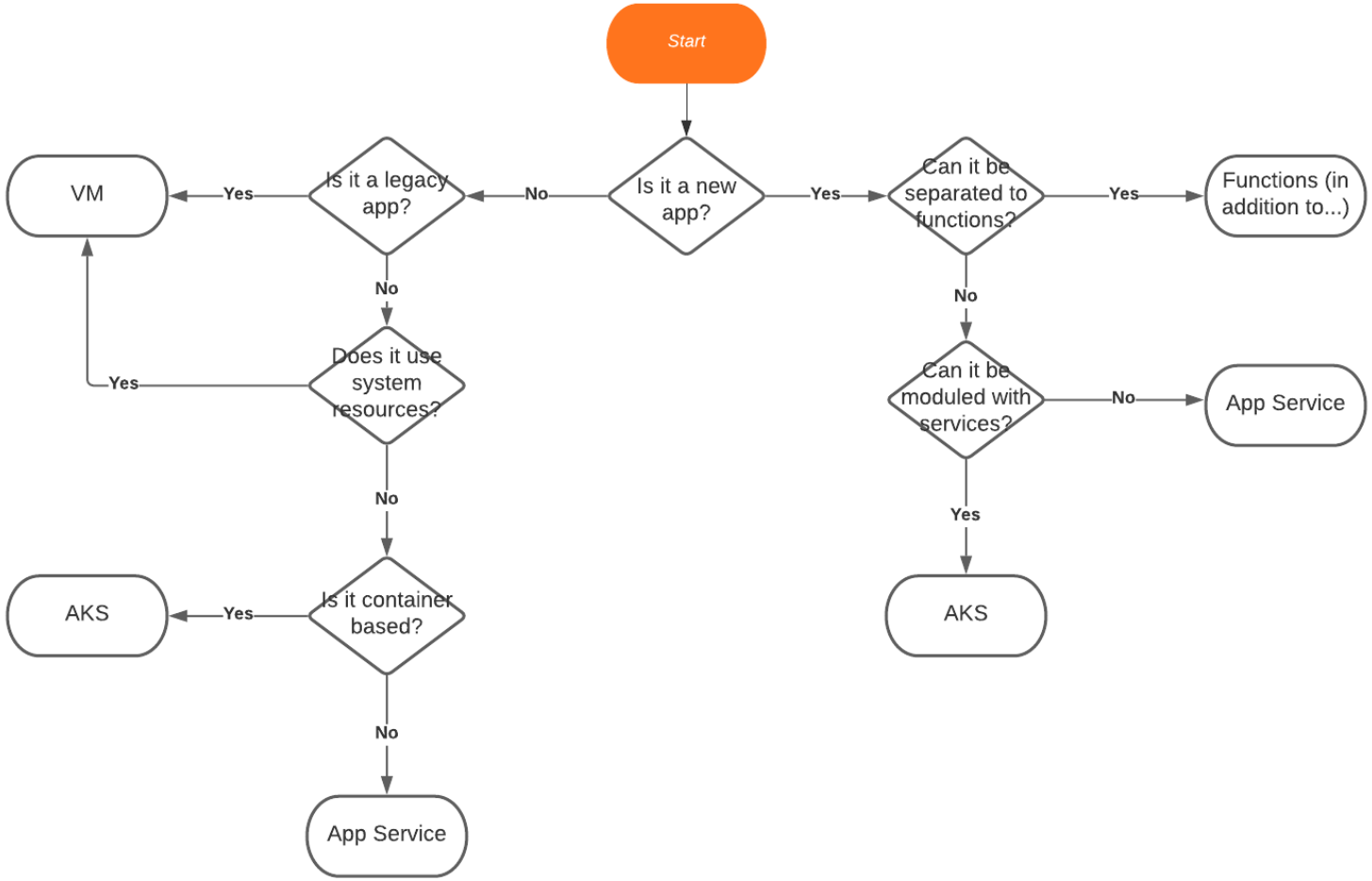
```
[FunctionName("Chaining")]
public static async Task<object> Run(
    [OrchestrationTrigger] IDurableOrchestrationContext context)
{
    try
    {
        var x = await context.CallActivityAsync<object>("F1", null);
        var y = await context.CallActivityAsync<object>("F2", x);
        var z = await context.CallActivityAsync<object>("F3", y);
        return  await context.CallActivityAsync<object>("F4", z);
    }
    catch (Exception)
    {
        // Error handling or compensation goes here.
    }
}
```

ReadIt!

Cloud Architecture



How to Choose Compute Type?



More Compute Options

- Logic Apps
- ACI – Azure Container Instance
- App Service Container – Deploy docker to App Service

Azure Networking

Memi Lavi
www.memilavi.com

Networking

- All aspects of networking in Azure
- Deals with resources' network connections, firewalls, etc.
- Might sound boring and not very important, but…

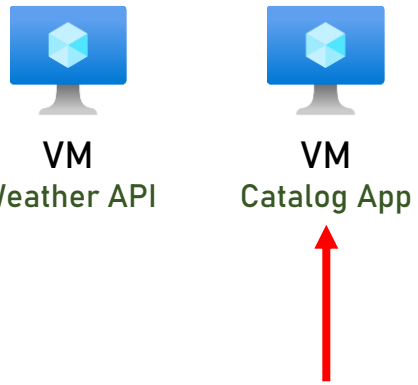
Networking is the foundation of cloud security

Cloud Architecture

A Word of Caution:

NEVER
leave a VM open to the internet this way

We will learn later on what should be done



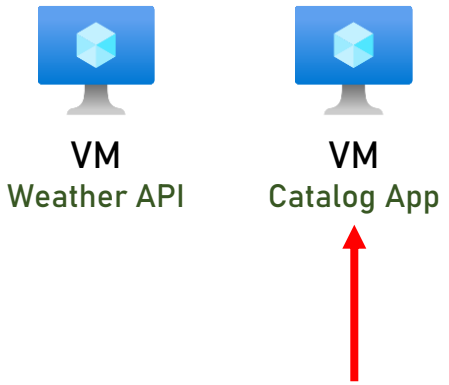
- Directly accessible from the internet
- Can be RDPed from anywhere

ReadIt!

Cloud Architecture

Two main threats:

- Brute force attacks on port 3389 (RDP)
- No line of defense in front of the VM web server



- Directly accessible from the internet
- Can be RDPed from anywhere

Networking knowledge is what makes a good cloud architect – an amazing cloud architect

Networking

- We'll talk about 4 networking-related cloud services:

VNets

SubNets

Load Balancer

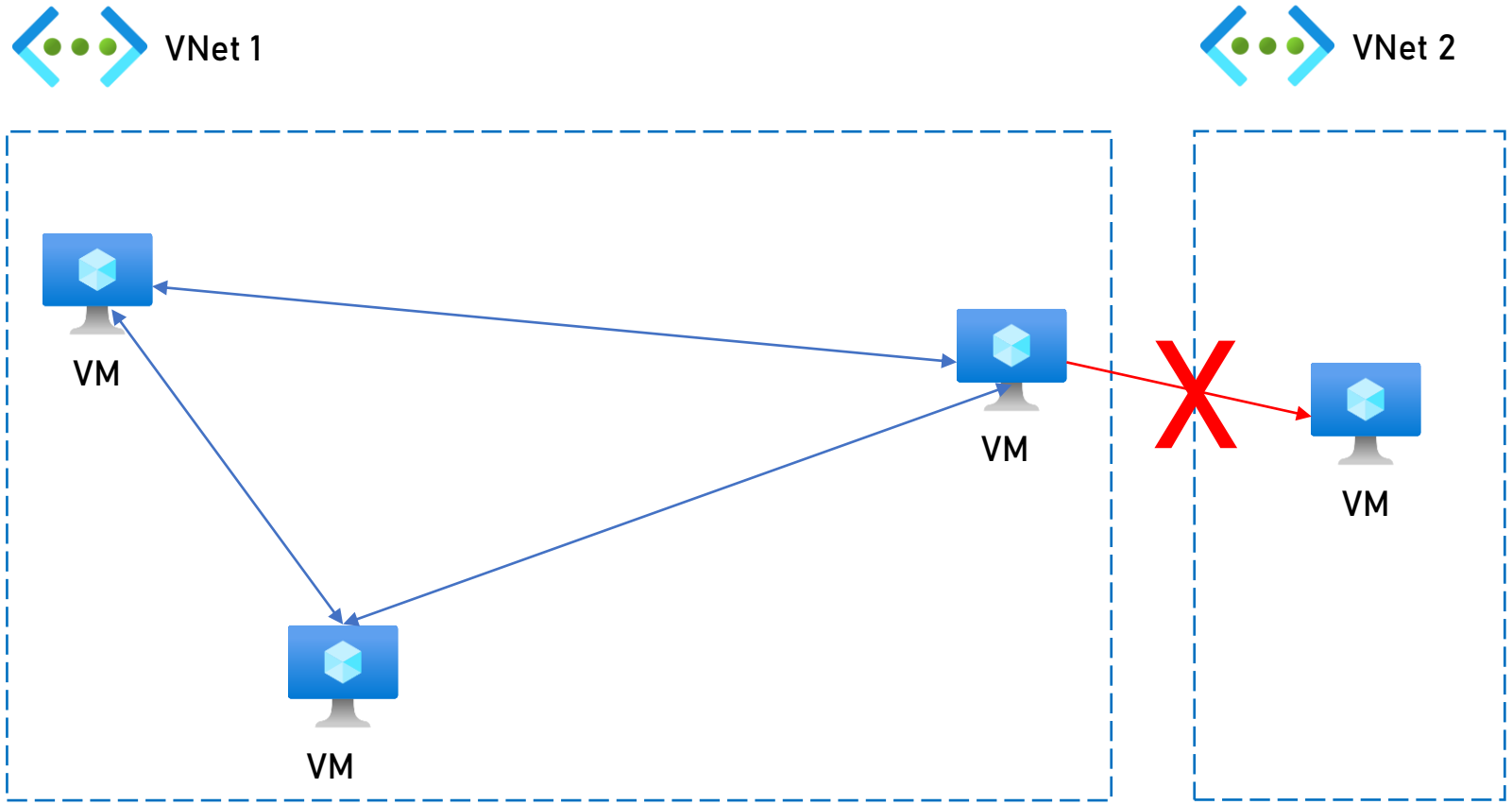
Application Gateway

Virtual Networks

- A network in which you can deploy cloud resources
- Many cloud resources are deployed within Vnets
  - VMs, App Services, DBs, etc.
- “Virtual” as in “based on physical network and logically separated from other virtual networks”

Virtual Networks

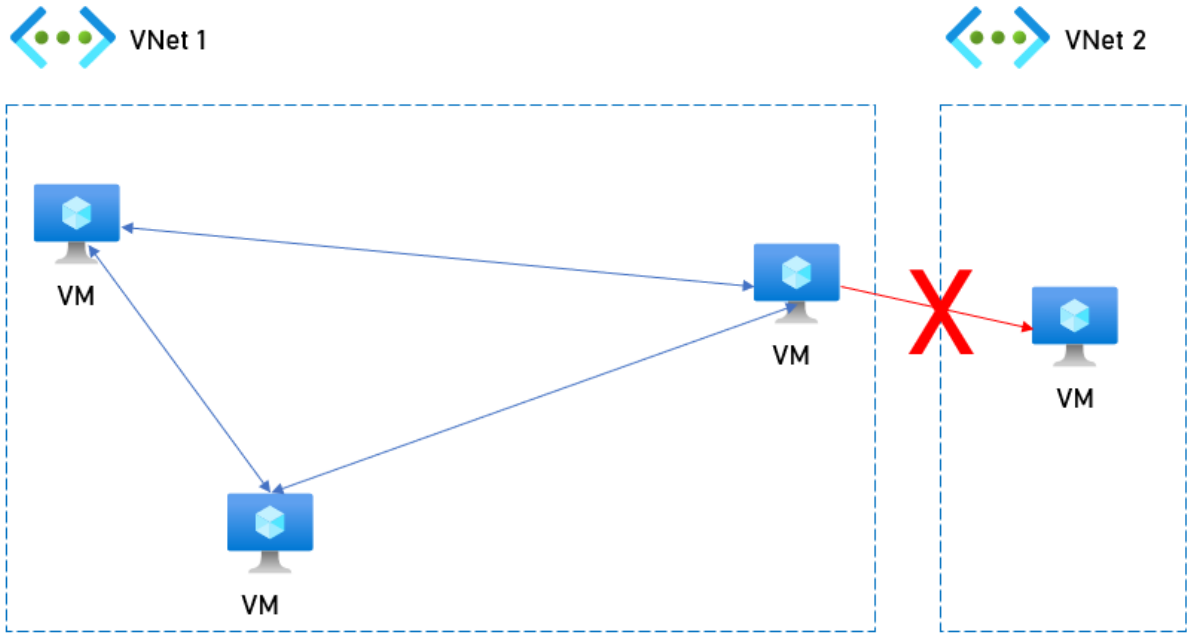
- Resources in VNet can communicate with each other by default



… but not with resources in other VNets

Virtual Networks

- Think of it as your organization's private network
- In AWS it's called VPC – Virtual Private Cloud
- Other organizations' VNets cannot communicate with your VNet



VNet Pricing

- VNets are free
- Limit of 50 VNets per subscription across all regions

Characteristics of VNets

- Scoped to a single Region
  - Cannot span multiple Regions
- Scoped to a single Subscription
- Can be connected via Peering
- Segmented using Subnets
- Protected using NSG (on the Subnets)

Security and VNets

- The most important thing to think about when designing network:

How to limit access to the resources in the VNet so that risk is minimized

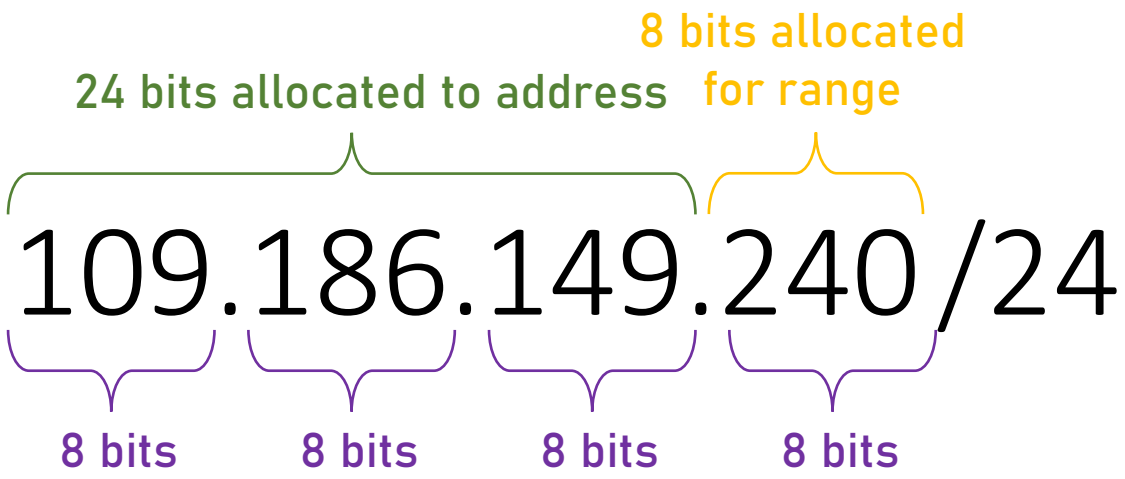
Addresses of VNets

- Each VNet has its own address range
  - Or IP Range
- By default – 65,536 addresses
- Can be customized
- All network devices must be in this address range
- Expressed using CIDR Notation

CIDR Notation

- Classless Inter-Domain Routing
- A method for representing an IP Range
- Composed of an address in the range and a number between 0 and 32
- The number indicates the number of bits that are allocated to the address. The smaller the number – the larger the range

CIDR Notation Example #1



109.186.149.000 – 109.186.149.255

256 Addresses

Bits refresher:
00000000 = 0
11111111=255

CIDR Notation Example #2

16 bits allocated to address

16 bits allocated for range

109.186.149.240/16

8 bits 8 bits 8 bits 8 bits

109.186.000.000 – 109.186.255.255

65,536 Addresses

Probably way too big…

Bits refresher:
00000000 = 0
11111111=255

CIDR Notation Example #3

149 Dec = 1001 ~~0101~~ Bin

1001 0000 Bin = 144 Dec

109.186.144.000 – 109.186.159.255

4,096 Addresses

Bits refresher:
00000000 = 0
11111111=255

CIDR Notation

- The good news:

You don't have to remember!

- A lot of CIDR calculators
  - ie. https://www.ipaddressguide.com/cidr

CIDR Notation

- More good news:
  - Azure usually shows the actual range

IPv4 address space	
192.168.0.0/16	192.168.0.0 - 192.168.255.255 (65536 addresses)

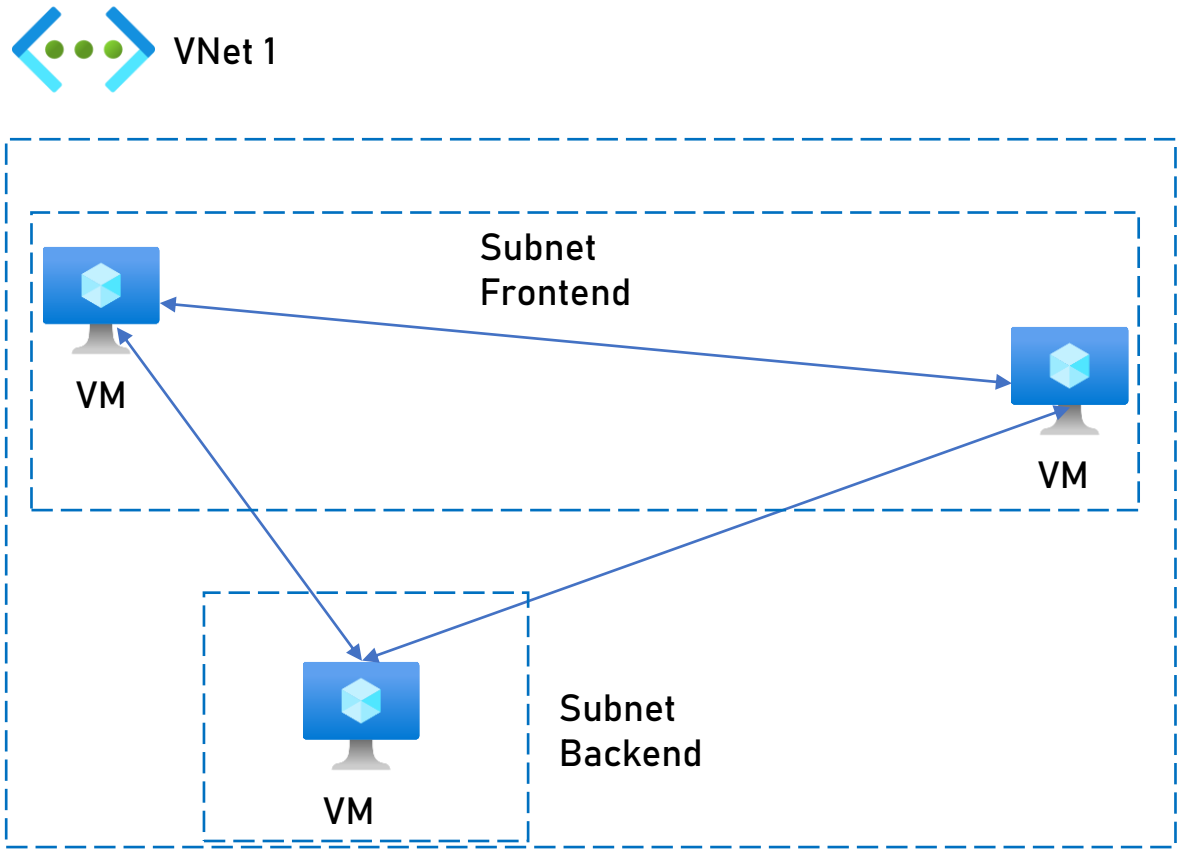
Subnet

- A logical segment in the VNet
- Shares a subset of the VNet's IP Range
- Used as a logical group of resources in the VNet
- Is a must. Resources must be placed in a Subnet, cannot be placed directly in the VNet

Subnet

- Resources in a subnet can talk to resources in other subnets in the same VNet*

*By default,
can be customized



Addresses of Subnets

- Each Subnet gets a share of the parent VNet's IP Range
- NEVER use the full range of the VNet in a Subnet
- Extremely hard to modify the range later
- Makes it hard to add future Subnets

Subnet Pricing

- Subnets are free
- Limit of 3,000 Subnets per VNet

Network Security Group

- Usually called NSG
- A gatekeeper for Subnets
- Defines who can connect in and out of subnet
- Think of it as a mini-firewall
- Should be a standard part of Subnet creation
- Is free

How NSG Works?

- Looks at 5 tuples:
  - Source (=Where did the connection come from)
  - Source Port (=The port the source is using)
  - Destination (=Where does the connection request goes)
  - Destination Port (=To which port does it want to connect)
  - Protocol (=TCP, UDP, Both)

How NSG Works?

- Based on these 5 tuples the connection is either allowed or denied
- This is called Security Rule
- Each rule is assigned a number
- The lower the number – the higher the priority of the rule

NSG and VMs

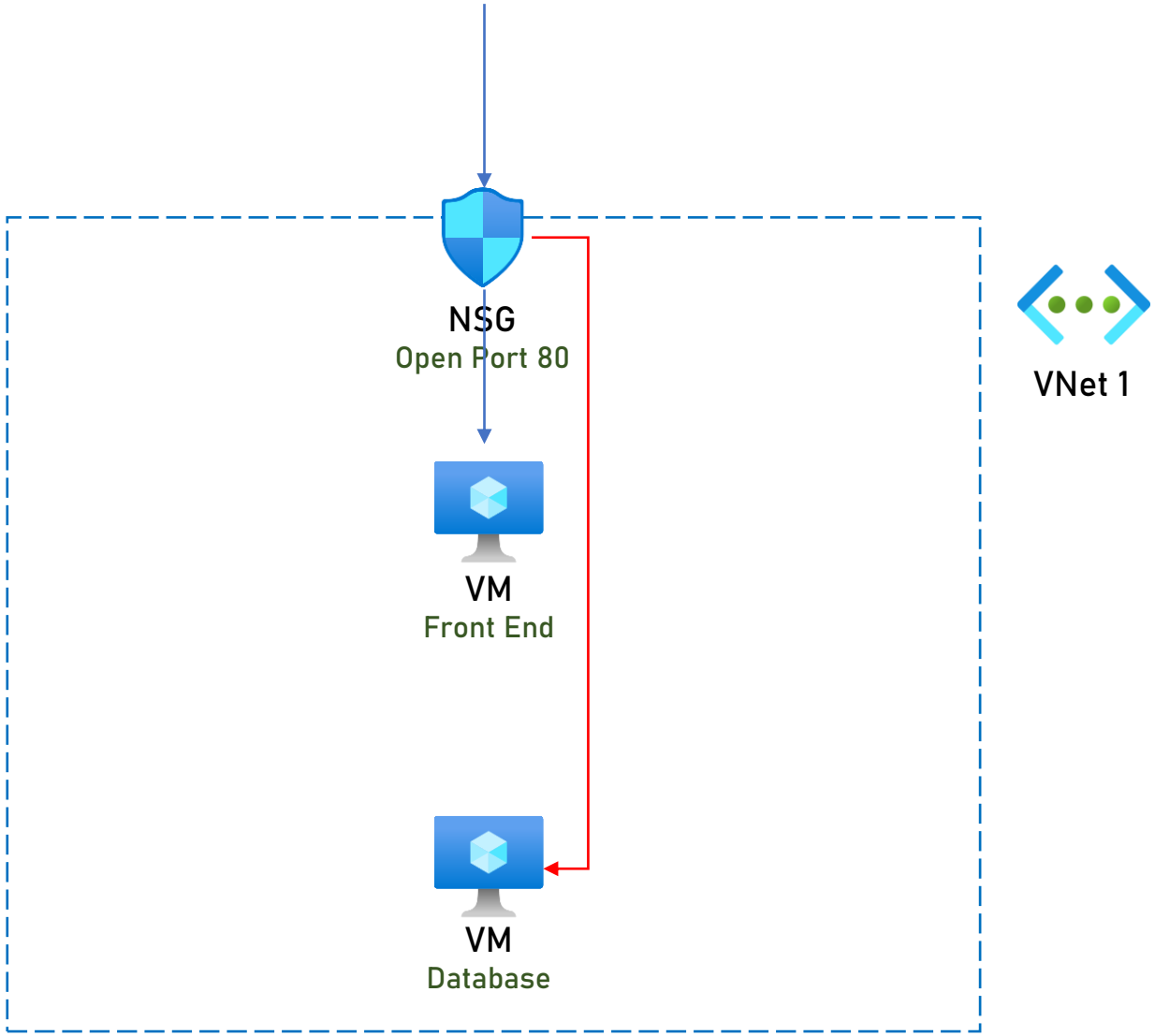
- An NSG is automatically created and attached to every newly-created VM's network interface
- By default – open RDP (on Windows) or SSH (on Linux) port to anyone
- MUST be handled first thing after creation

Network Peering

- Sometimes, to increase security, we want to place some resources in a completely different VNet
  - Not just Subnet!
- Examples:
  - Separate systems
  - System layers
  - Sensitive databases

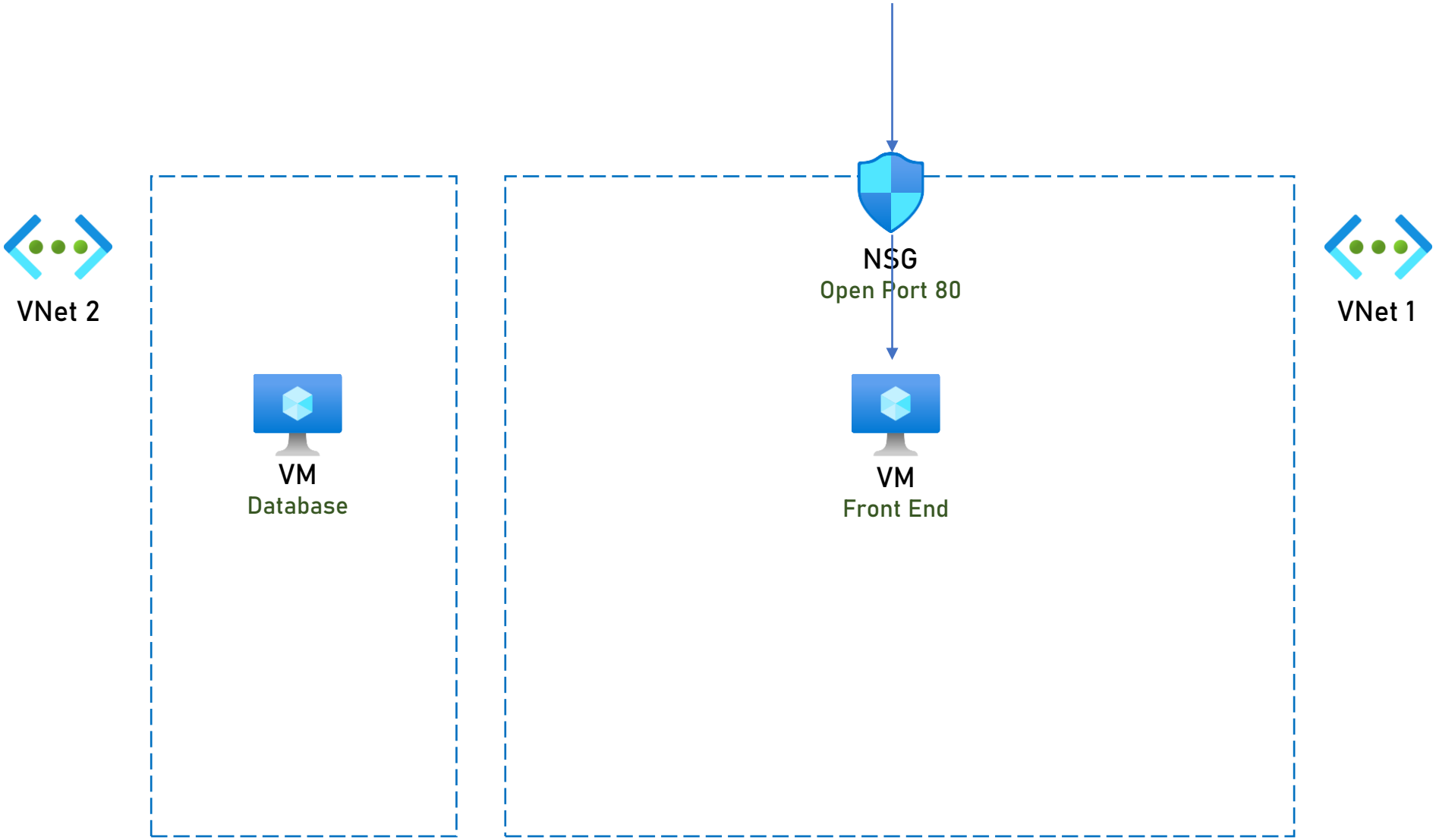
Network Peering

- Main reasoning:
  - Not to place non-public resources in a VNet that has public access



Network Peering

- So…



Network Peering

- But…

Network Peering

- Allows two VNets to connect to each other
- From the user's point of view it's a single VNet
- Make sure address spaces are not overlapped!
- Use NSG for protection
- Can work across Regions

Network Peering

- Not free

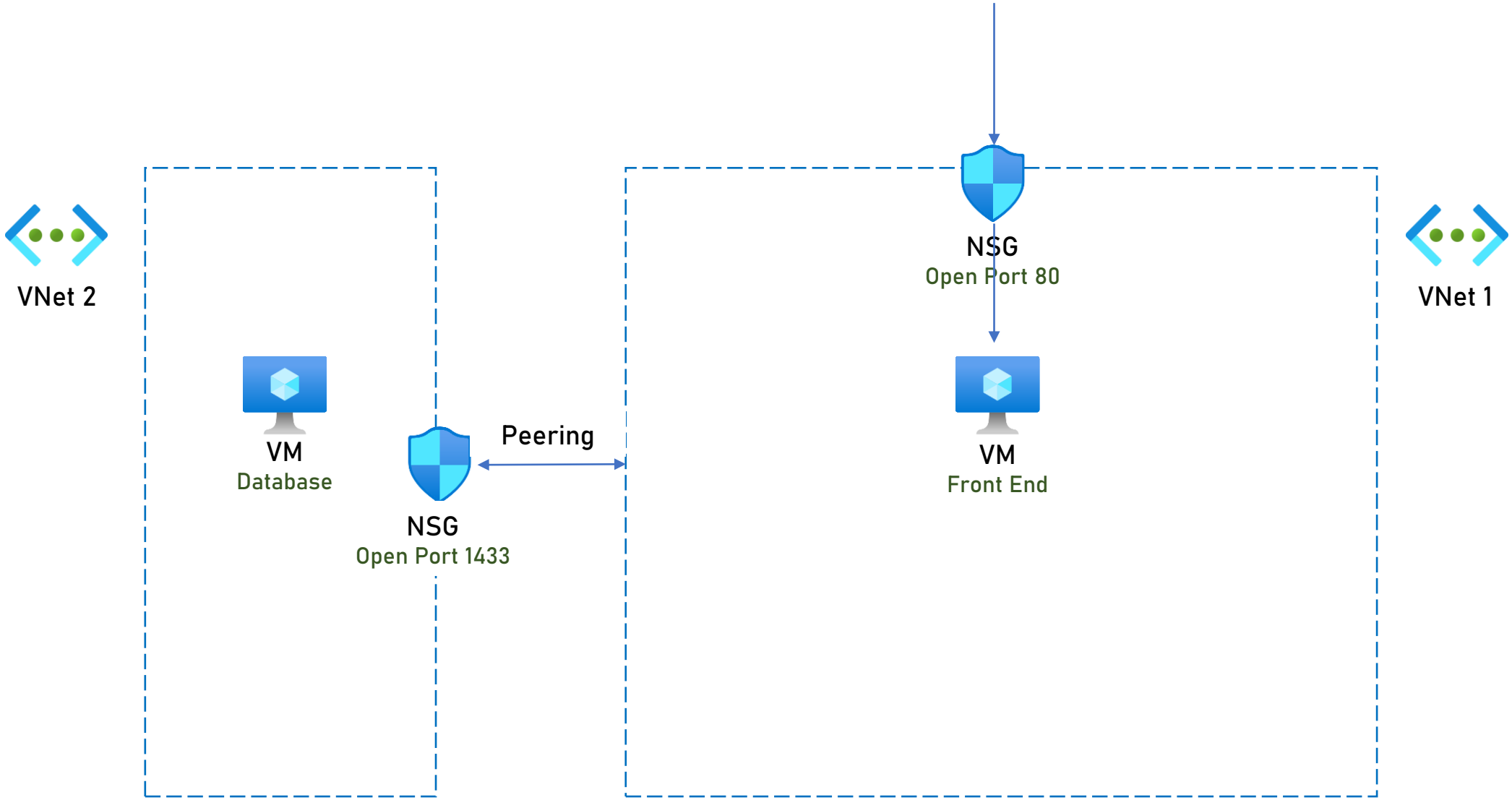
Outbound data transfer

100 GB	×	$0.0100 Per GB

Inbound data transfer

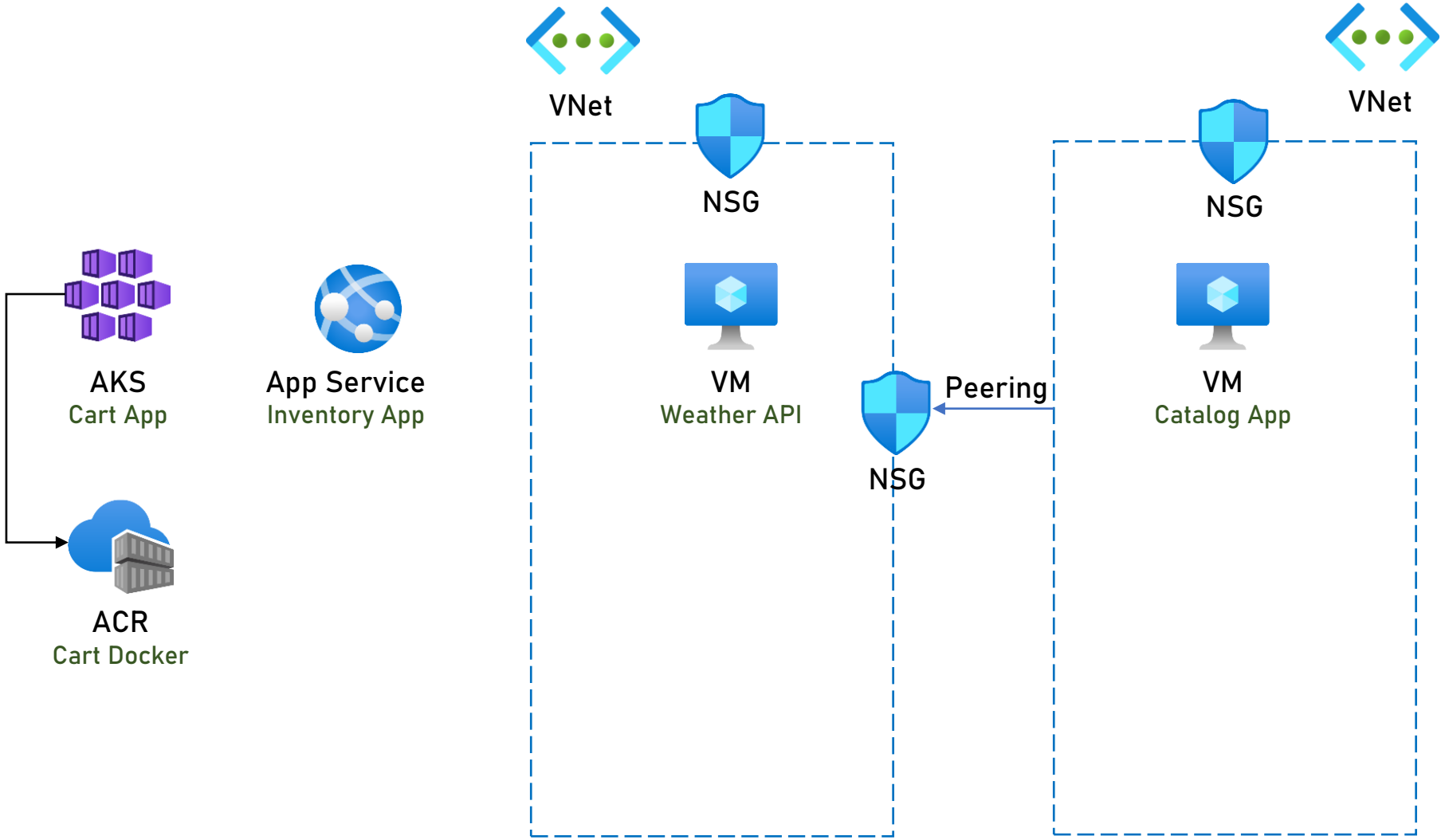
100 GB	×	$0.0100 Per GB

Network Peering



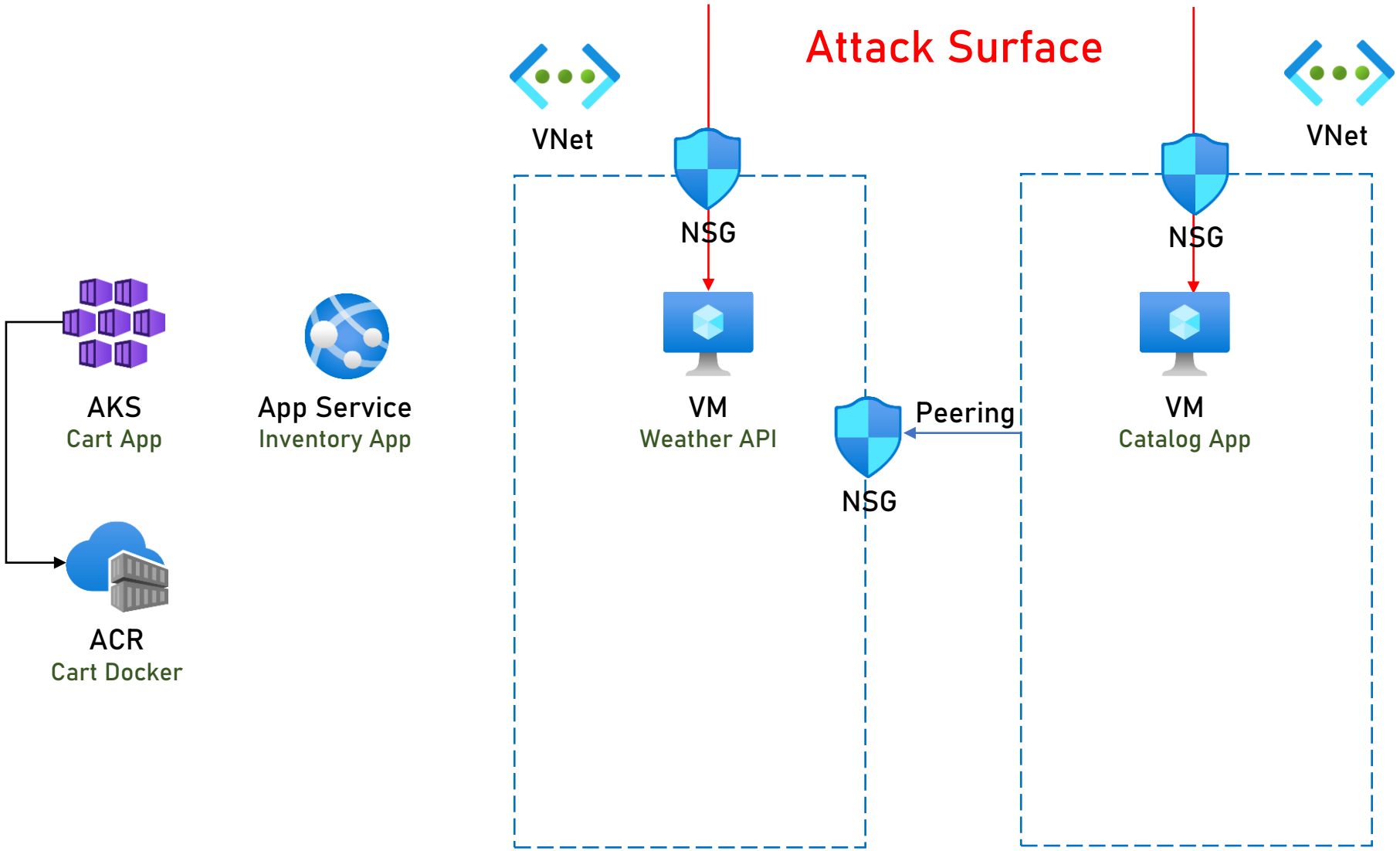
ReadIt!

Cloud Architecture



ReadIt!

Cloud Architecture



Secure VM Access

- The larger the attack surface – the greater the risk
- We want to minimize it as much as possible
- Leaving public IPs open is always a risk we want to avoid
- Not directly related to the app design but important nonetheless

Secure VM Access

- What can be done?

JIT Access

VPN

Jump Box

Bastion

JIT Access

- Just In Time Access
- Opens the port for access on demand, and automatically closes it
- Rest of the time – it's closed
- Can be configured from the VM's page in the portal
- Requires Security Center License Upgrade

VPN

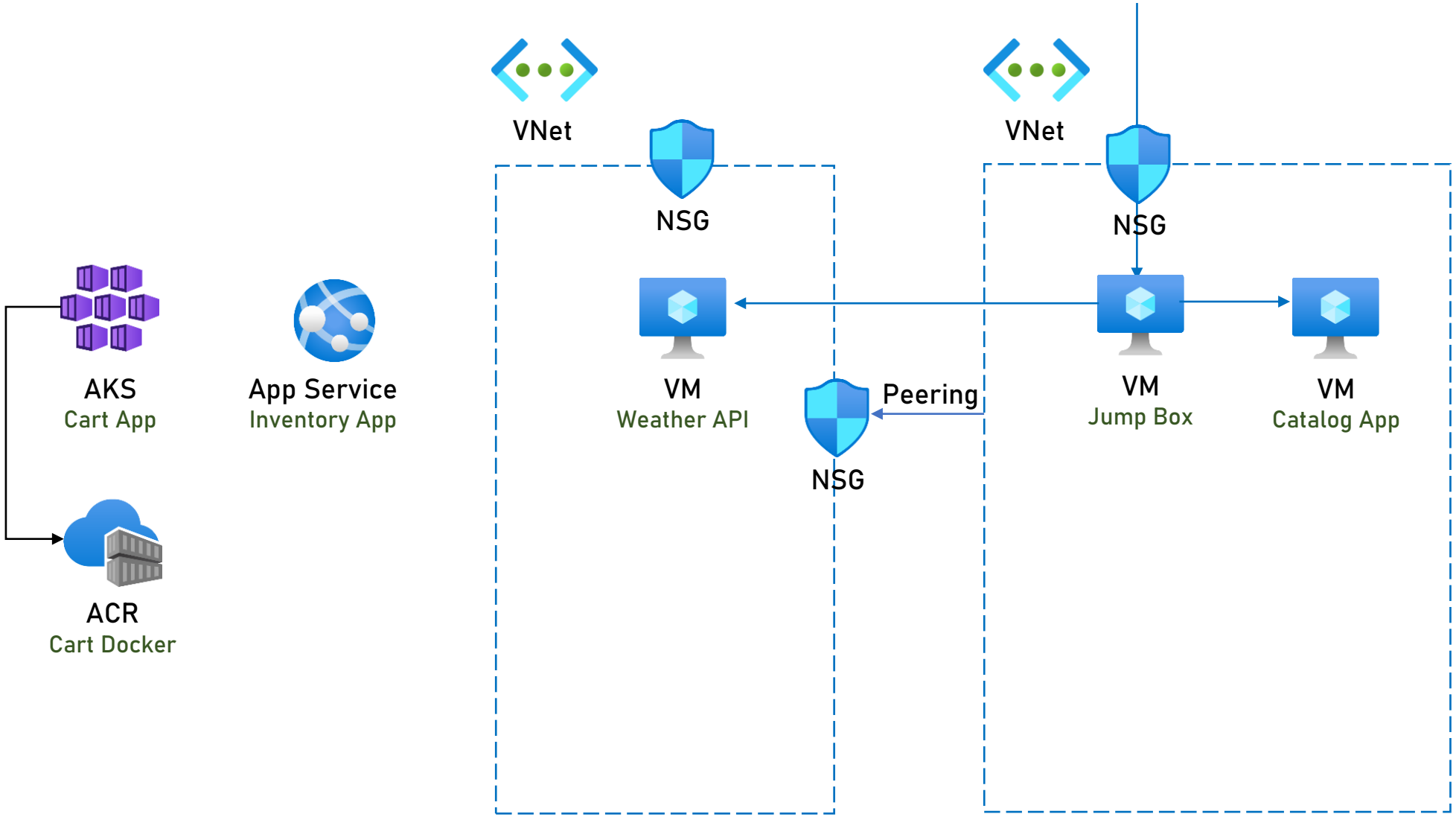
- A secure tunnel to the VNet
- Can be configured so that no one else can connect to the VNet
- Requires VPN software and license (not part of Azure)

Jump Box

- Place another VM in the VNet
- Allow access ONLY to this VNet
- When need to access one of the other VMs – connect to this one and connect from it to the relevant VM
- Only one port is open (still kind of a problem…)
- Cost: The additional VM (the Jump Box)

ReadIt!

Cloud Architecture



Bastion

- A web-based connection to the VM
- No open port is required
- Simple and secure
- Cost: ~140$ / month

Bastion Downsides

- Cost
- Requires portal access
  - This is said to be handled by the Bastion team ☺

Service Endpoint

- A lot of managed services expose public IP
  - ie. Azure SQL Server, App Services, Storage and more
- Sometimes these resources are accessed only from resources in the cloud
  - ie. Database in the backend
- Might pose a security risk

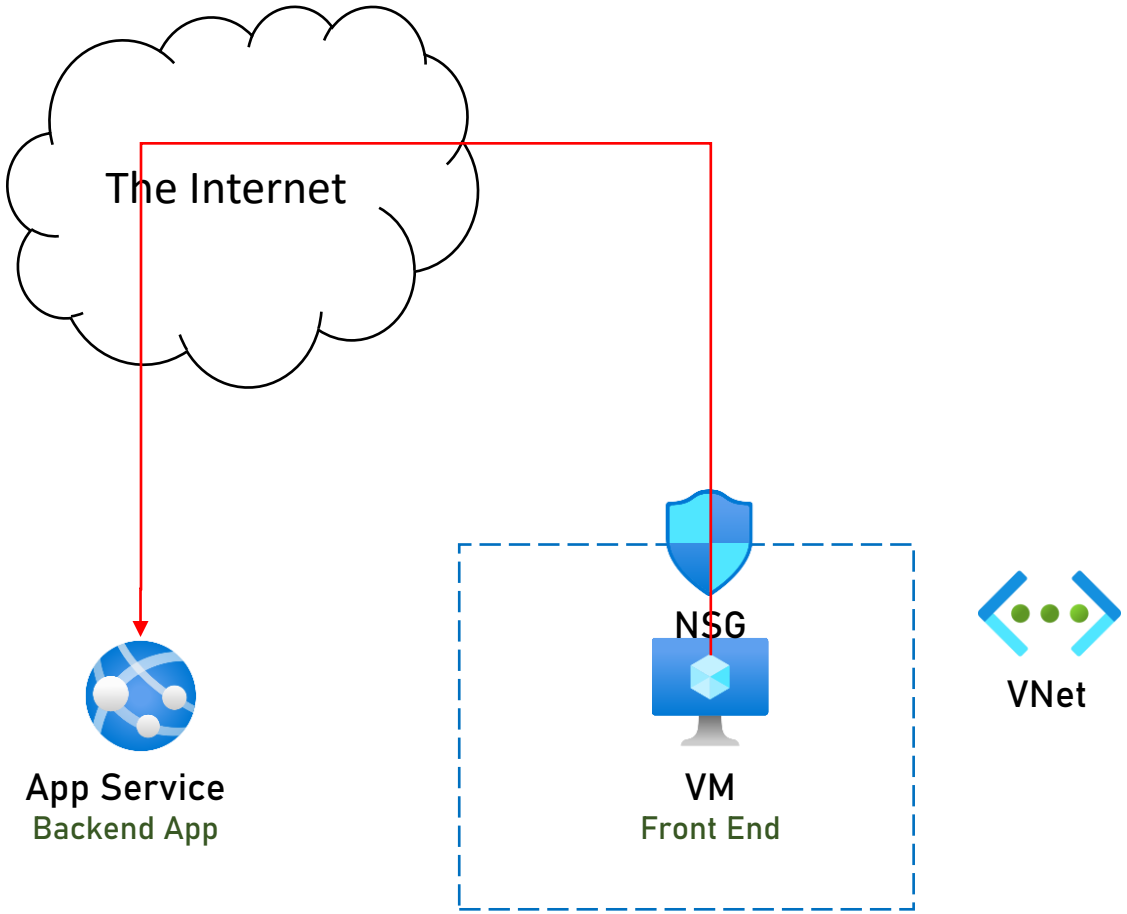
Service Endpoint

- Service Endpoint solves this security risk
- Creates a route from the VNet to the managed service
- The traffic never leaves Azure backbone
  - Although the resource still has a public IP
- Access from the internet can be blocked
- Is free!

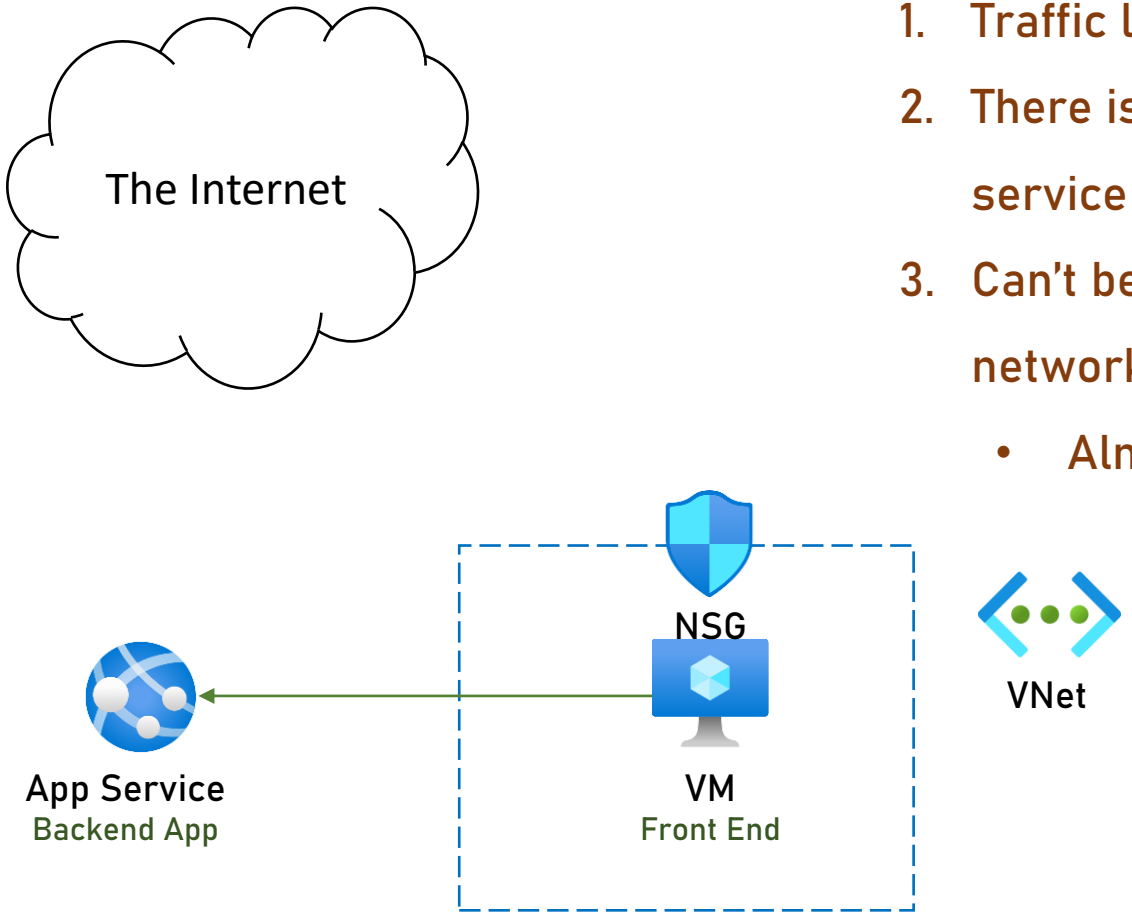
Service Endpoint

- How it's done:
  - Enable Service Endpoint on the Subnet from which you want to access the resource
  - On the resource, set the subnet as the source of traffic
  - Voila!

Without Service Endpoint



With Service Endpoint



Note:

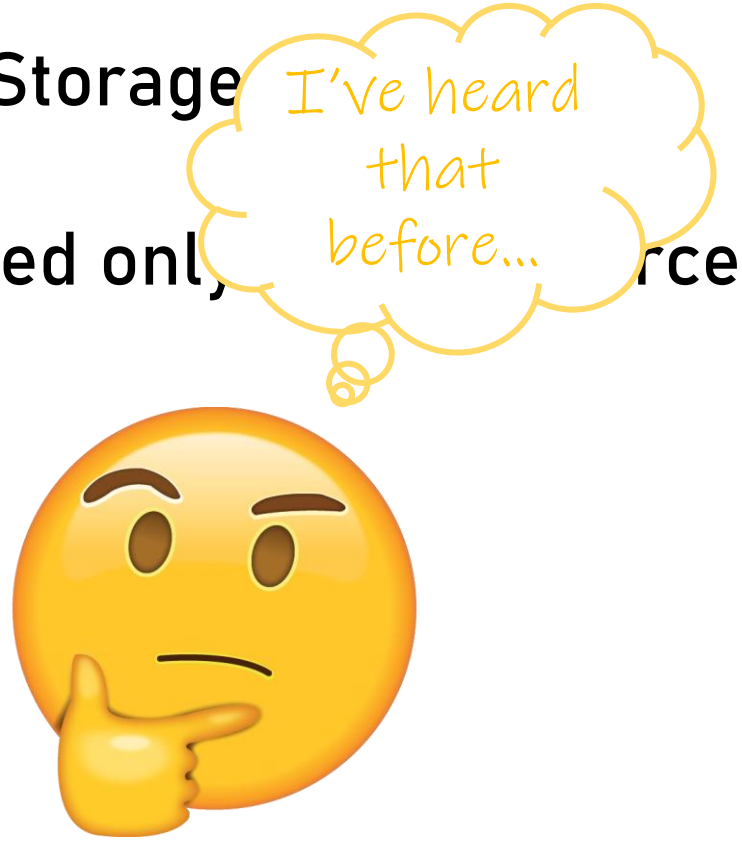
1. Traffic leaves the VNet
2. There is a public IP on the PaaS service (App Service)
3. Can't be used from on-prem network
   - Almost…

Service Endpoint

- Resources support Service Endpoint:
  - Storage
  - SQL Database
  - Synapse Analytics
  - PostgreSQL
  - MySQL
  - Cosmos DB
  - KeyVault
  - Service Bus
  - Event Hub
  - App Service
  - Cognitive Services

Private Link

- A lot of managed services expose public IP
  - ie. Azure SQL Server, App Services, Storage
- Sometimes these resources are accessed only [illegible]rces in the cloud
  - ie. Database in the backend
- Might pose a security risk



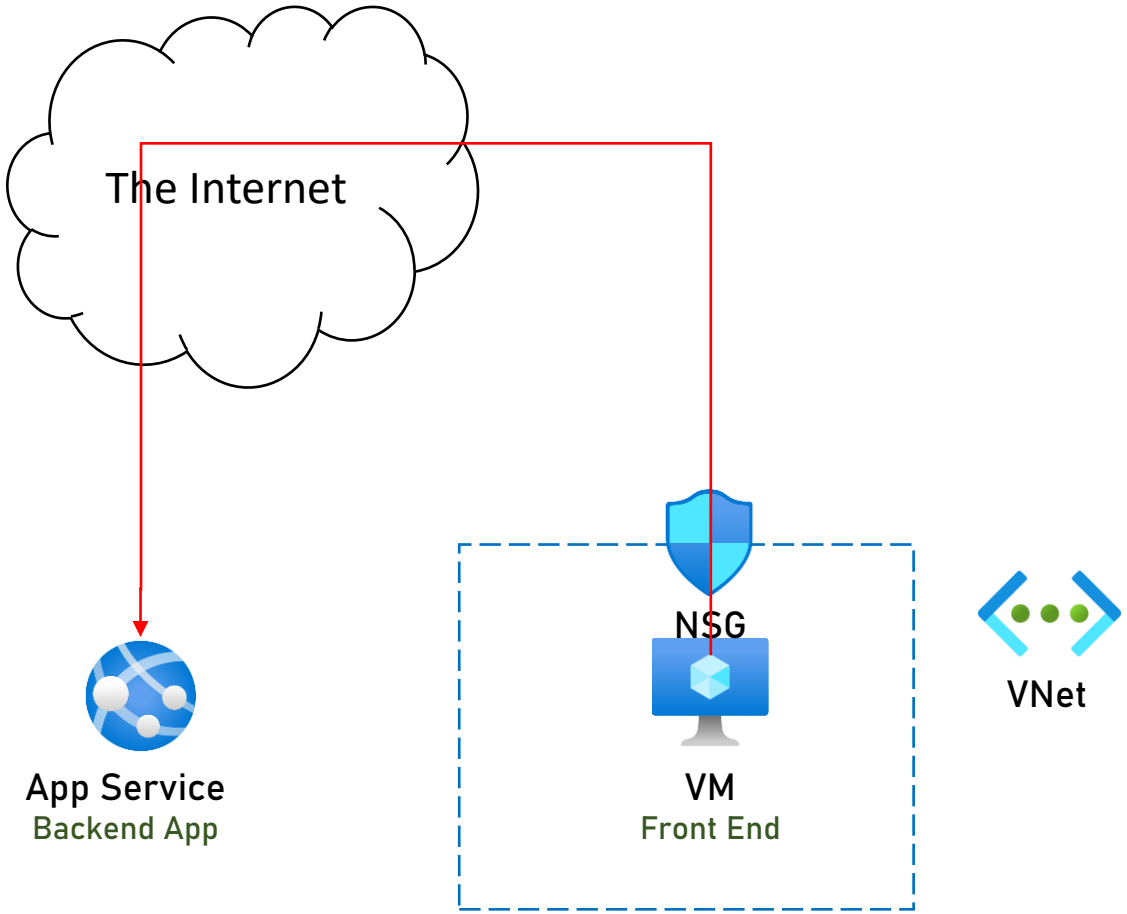
Private Link

- A newer solution to this problem
- Extends the managed service into the VNet
- The traffic never leaves the VNet
- Access from the internet can be blocked
- Can be used from on-prem networks
- Isn't free

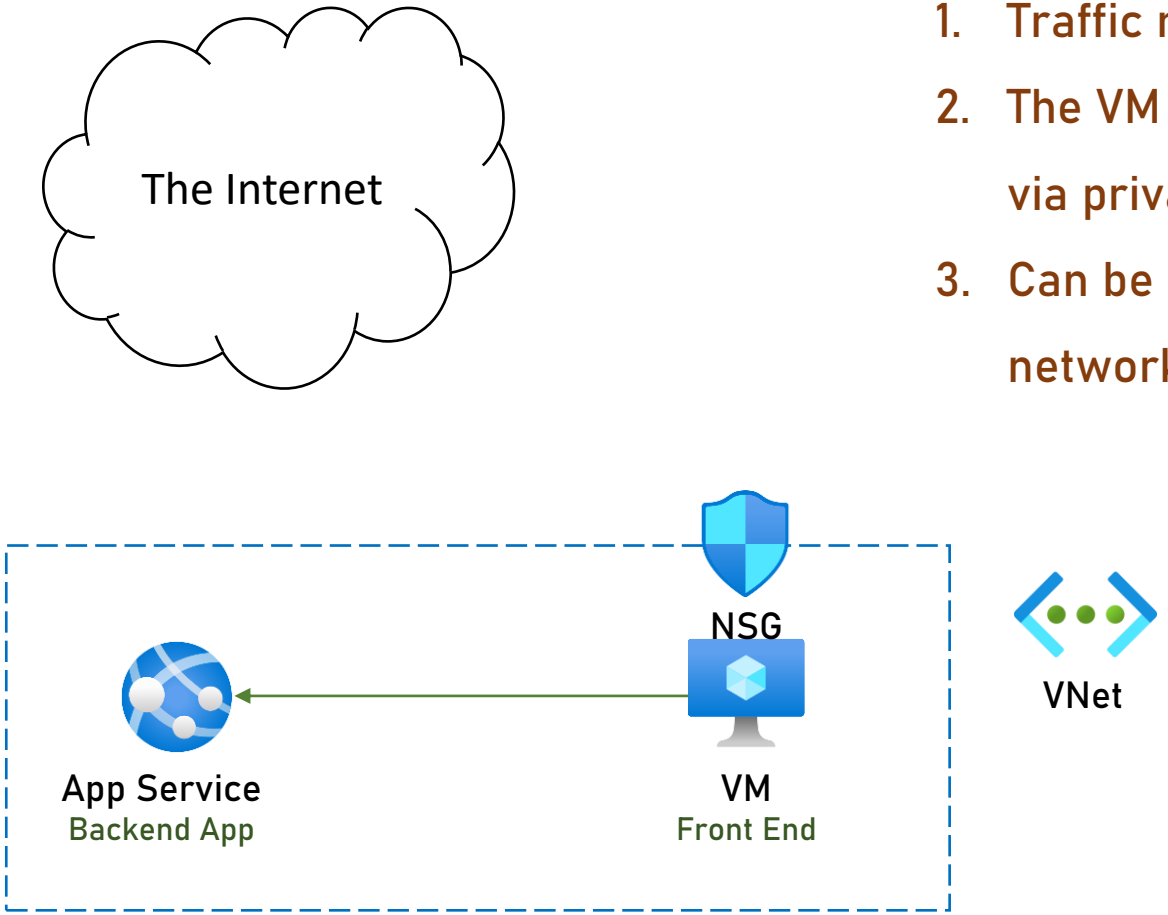
Private Link

- How it's done:
  - Configure the resource to connect to the VNet
  - Configure private DNS
    - Might cause a problem if you have your own DNS

Without Private Link



With Private Link



Note:

1. Traffic never leaves the VNet
2. The VM talks to the App Service via private IP
3. Can be used from on-prem network

Private Link

- Resources support Private Link:
  - Storage
  - SQL Database
  - Synapse Analytics
  - PostgreSQL
  - MySQL
  - Cosmos DB
  - KeyVault
  - Redis
  - AKS
  - Search
  - ACR
  - App Configuration
  - Backup
  - Service Bus
  - Event Hub
  - Monitor
  - Relay
  - Event Grid
  - App Service
  - Machine Learning
  - Automation
  - IOT Hub
  - SignalR
  - Batch

Service Endpoint vs Private Link

	Service Endpoint	Private Link
Security	Connects via Public IP	Connects via Private IP
Simplicity	Very simple	More complex
Price	Free	Not free
Supported services	Limited list	Large list, probably will get larger
On-Prem connectivity	Quite complex	Supported

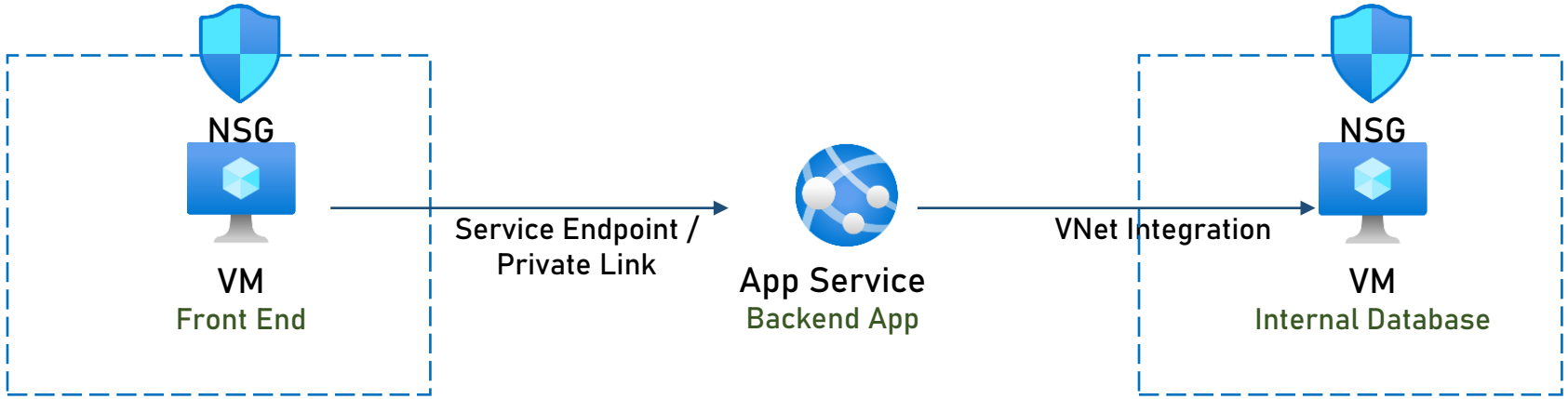
Service Endpoint vs Private Link

- We'll demonstrate Service Endpoint and Private Link later
  - Service Endpoint – on Application Gateway and Azure SQL Server
  - Private Link – on KeyVault

App Service VNet Integration

- Allows access from App Service to resources within VNet
  - So that these resources should not be exposed on the internet
- Extremely useful when App Service needs access to a VM with some internal resources
- Supports same-region VNets. For VNets in other regions – a gateway is required

SE / PL vs VNet Integration



App Service Access Restrictions

- Similar to NSG – but for App Services
- Restricts traffic to the App Service
- By default – all inbound traffic is allowed (in relevant ports)
- Using access restrictions inbound traffic is restricted to the allowed IPs / VNets / Service Tag

App Service Access Restrictions

- Main use cases:
  - Backend App Service that should be accessed from front end App Service / VM only
  - App Service that sits behind Application Gateway / Load Balancer and shouldn't be accessible directly
  - Open App Service to a specific customer only

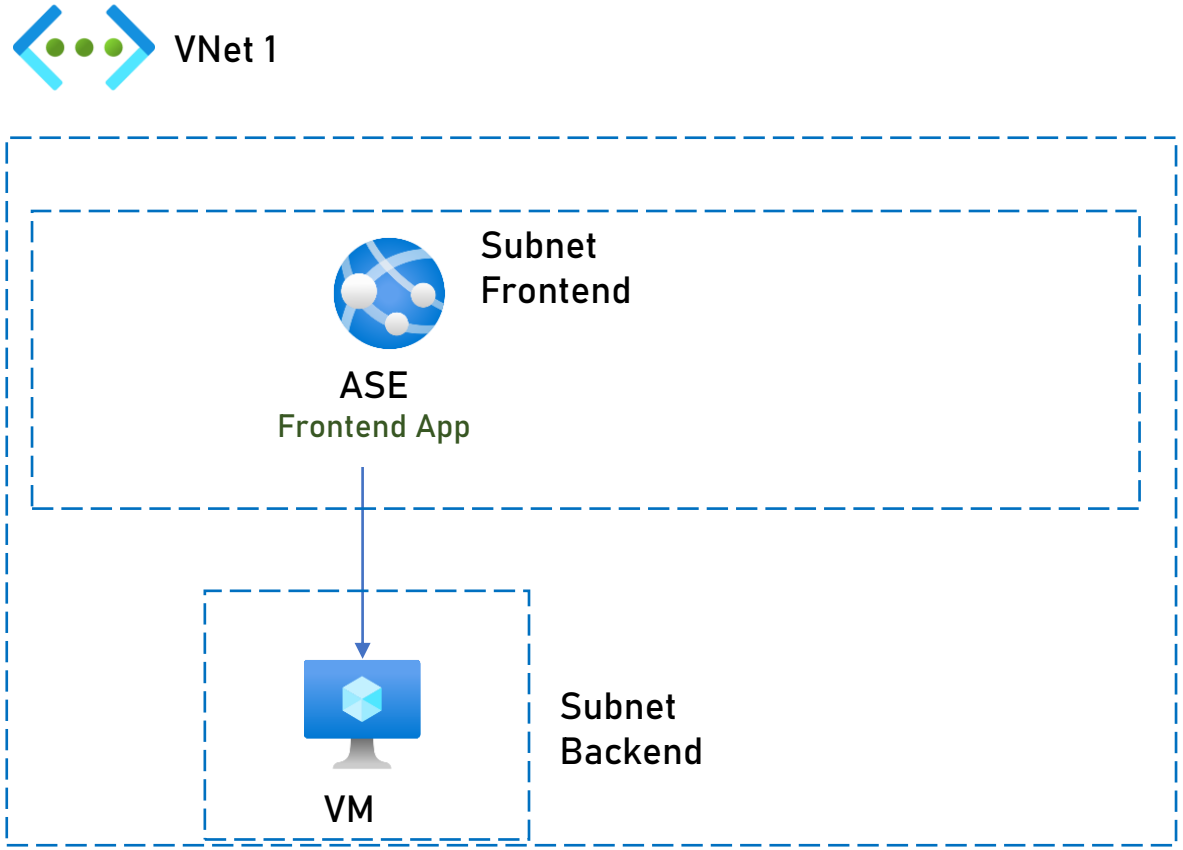
ASE

- App Service Environment
- Special type of app service deployed directly to a dedicated VNet
- VNet can be configured like any other VNet – Subnets, NSGs, etc
- Created on dedicated hardware
- Quite expensive…

ASE

- Major use cases:
  - Elevated security – complete isolation
  - Very high scale requirements

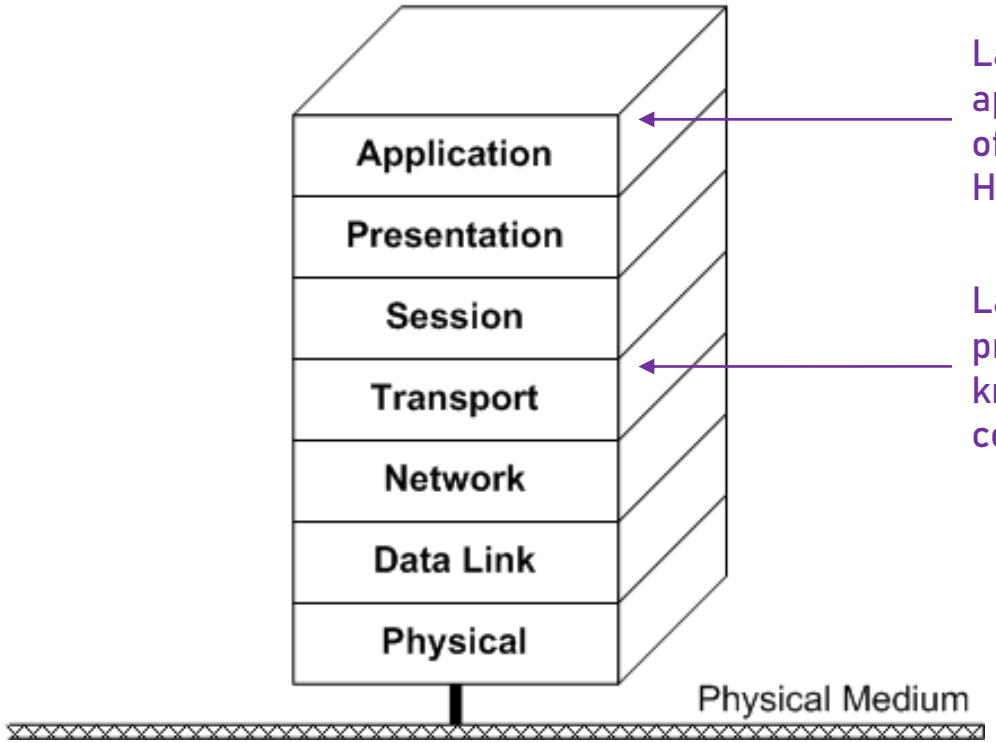
ASE



Load Balancer

- Azure service that distributes load and checks health of VMs
- When a VM is not healthy – no traffic is directed to it
- Can work with VMs or Scale Set
- Can be public or private
- Operates at layer 4 of the OSI model

7 Layers Model

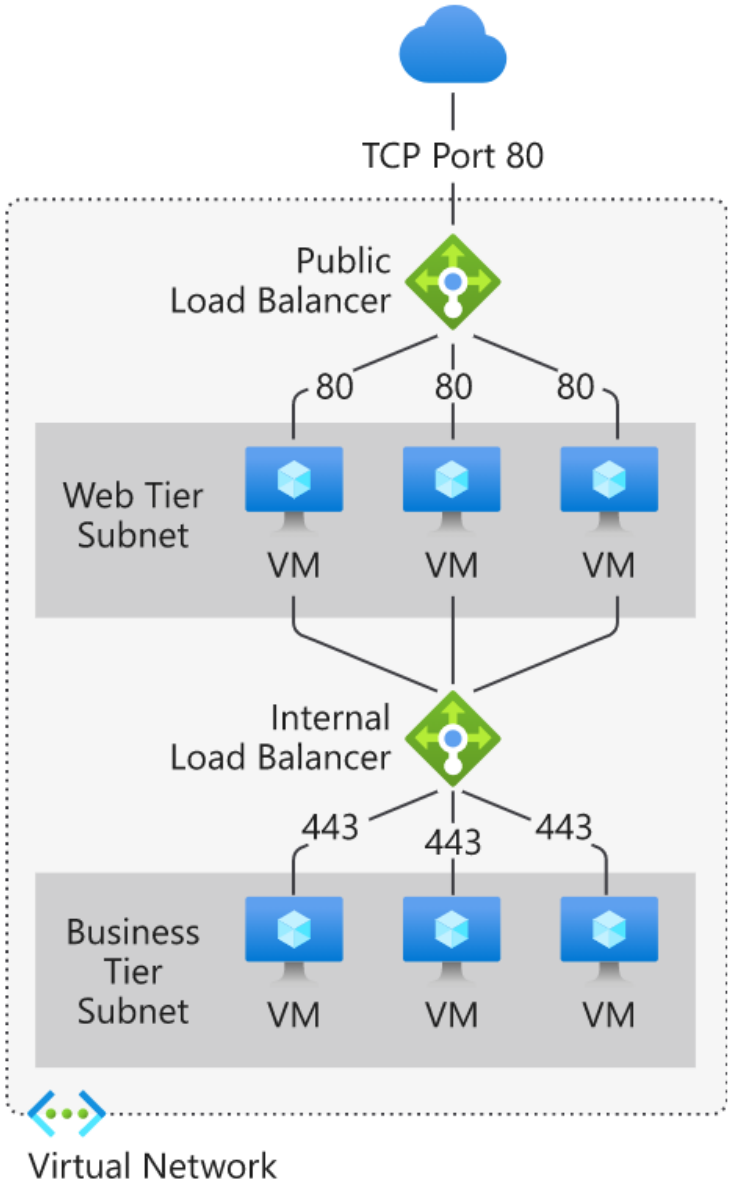


Layer 7: Interacts with the application. Can see the content of the transmission. Example: HTTP URL + path + params

Layer 4: Knows about IP, Port, protocol, TLS and more. Has no knowledge about the actual content

Source: https://docs.microsoft.com/en-us/windows-hardware/drivers/network/windows-network-architecture-and-the-osi-model

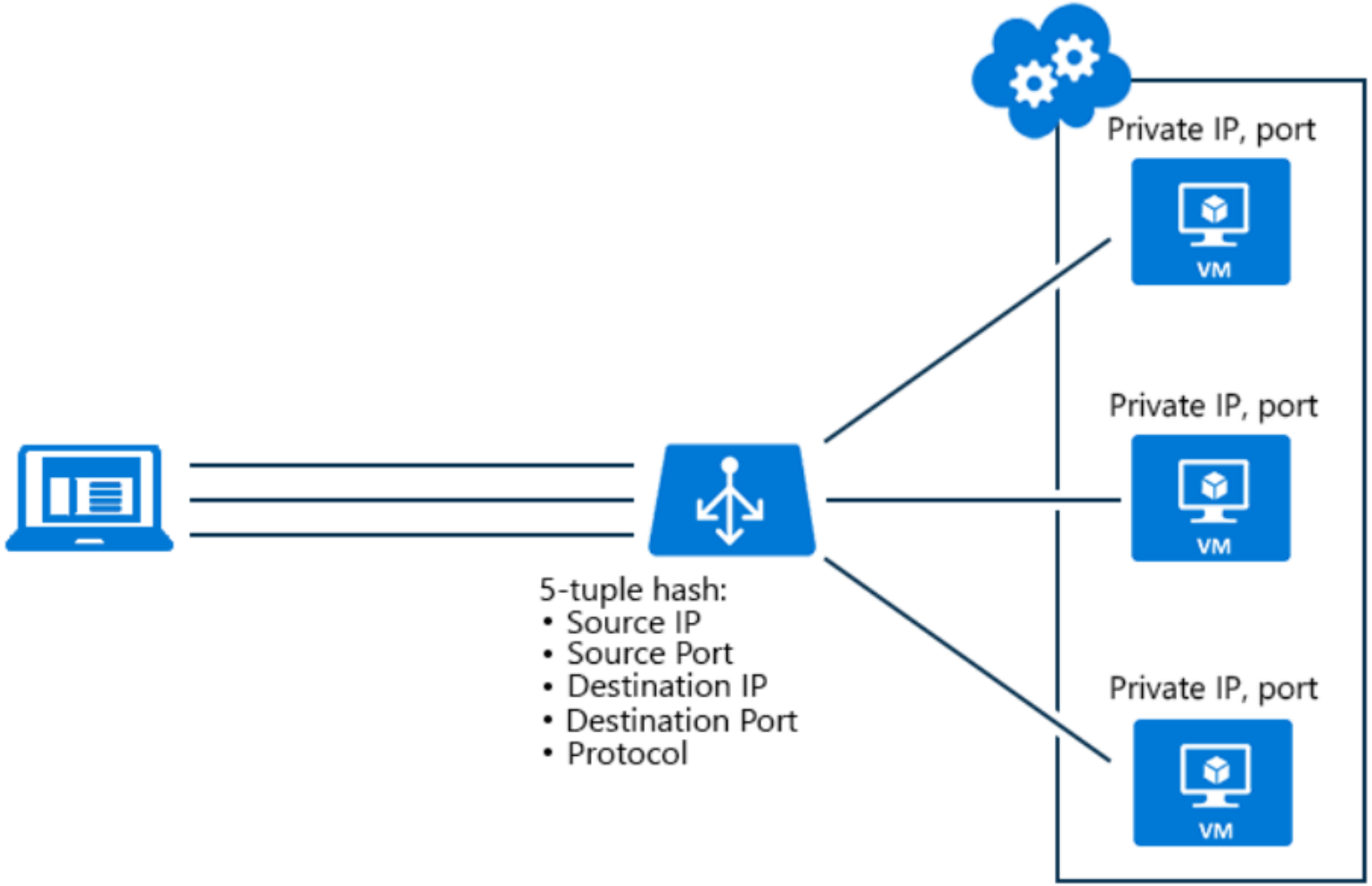
Load Balancer



Load Balancer Distribution Algorithm

- Based on 5 tuple hash:
  - Source IP
  - Source port
  - Destination IP
  - Destination port
  - Protocol type
- Same tuples used by NSG

Load Balancer Distribution Algorithm



Load Balancer Types

Basic	Standard

Load Balancer Types

Basic	Standard
No redundancy	Redundant

Load Balancer Types

Basic	Standard
No redundancy	Redundant
Open by default	Secure by default

Load Balancer Types

Basic	Standard
No redundancy	Redundant
Open by default	Secure by default
Up to 300 instances	Up to 1000 instances

Load Balancer Types

Basic	Standard
No redundancy	Redundant
Open by default	Secure by default
Up to 300 instances	Up to 1000 instances
No SLA	99.99% SLA

Load Balancer Types

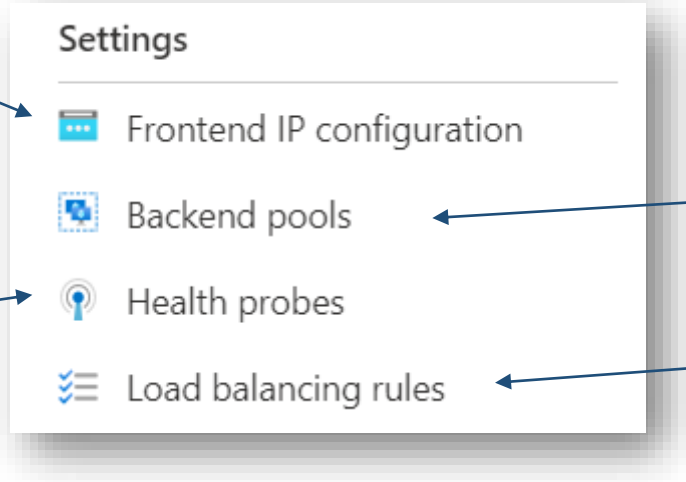
Basic	Standard
No redundancy	Redundant
Open by default	Secure by default
Up to 300 instances	Up to 1000 instances
No SLA	99.99% SLA
Free	Not Free

Configuring Load Balancer

- 4 main configurations:

The public IP exposed by the Load Balancer

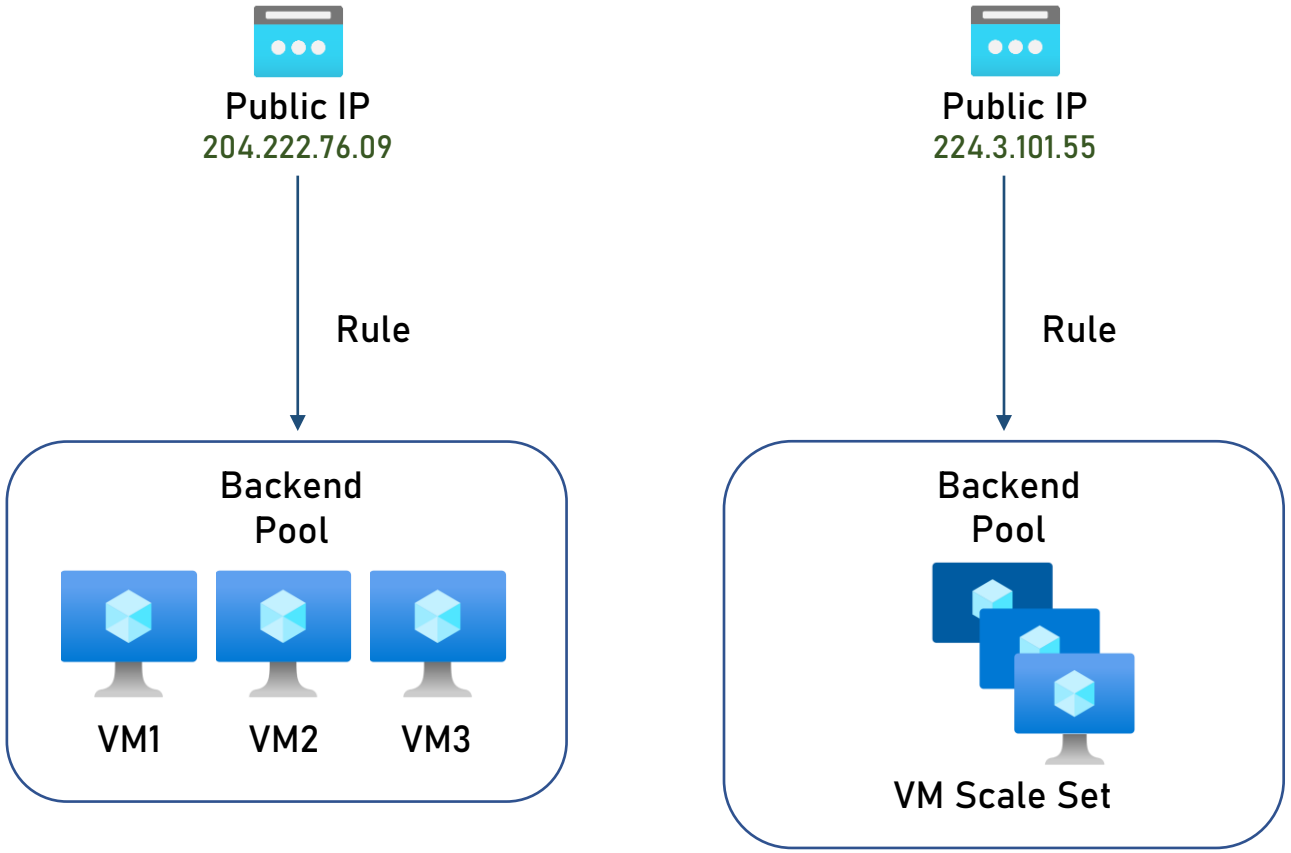
Probes checking the health of the VMs. Non-healthy VM will not be routed to

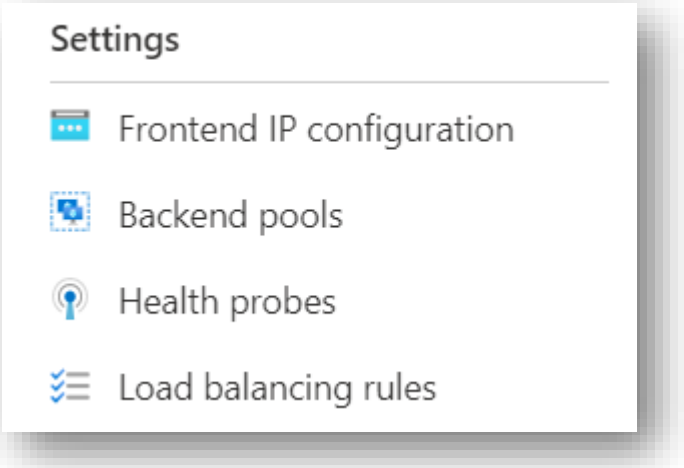


The VMs connected to the Load Balancer

A rule connecting Frontend IP with Backend pool

Example


Public IP
204.222.76.09
Rule
Backend Pool
VM1
VM2
VM3
Public IP
224.3.101.55
Rule
Backend Pool
VM Scale Set


Settings
Frontend IP configuration
Backend pools
Health probes
Load balancing rules

Health Probes

- Check the health of the VM
- A non-healthy VM will be marked as Down and will not be routed to
- Run in intervals (usually a few seconds)
- Can run on TCP, HTTP, HTTPS (Standard only)
- Configurable unhealthy threshold – how many times a check should fail for the VM to be marked as Down (default is 2)

Health Probes

Add health probe

mylb

Name *

Protocol

TCP

Port *

80

Interval *

5

seconds

Unhealthy threshold *

2

consecutive failures

Health Probes

- Run on the VM's host
- No network traffic outside the host
- Originate from the same IP: 168.63.129.16
- Allowed by default in NSG

Inbound port rules | Outbound port rules | Application security groups | Load balancing

Network security group az-vnet-test2-nsg (attached to network interface: az-vnet-test2665)
Impacts 0 subnets, 1 network interfaces

Add inbound port rule

Priority	Name	Port	Protocol	Source	Destination	Action
300	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

When to Use Load Balancer

- Great for internal resources
- Do not use for external resources
  - Especially on Web Apps / Web API / etc.
  - Can't handle HTTP
  - Doesn't route based on path
  - No protection
- For this we have the Application Gateway
  - And demo too…

Application Gateway

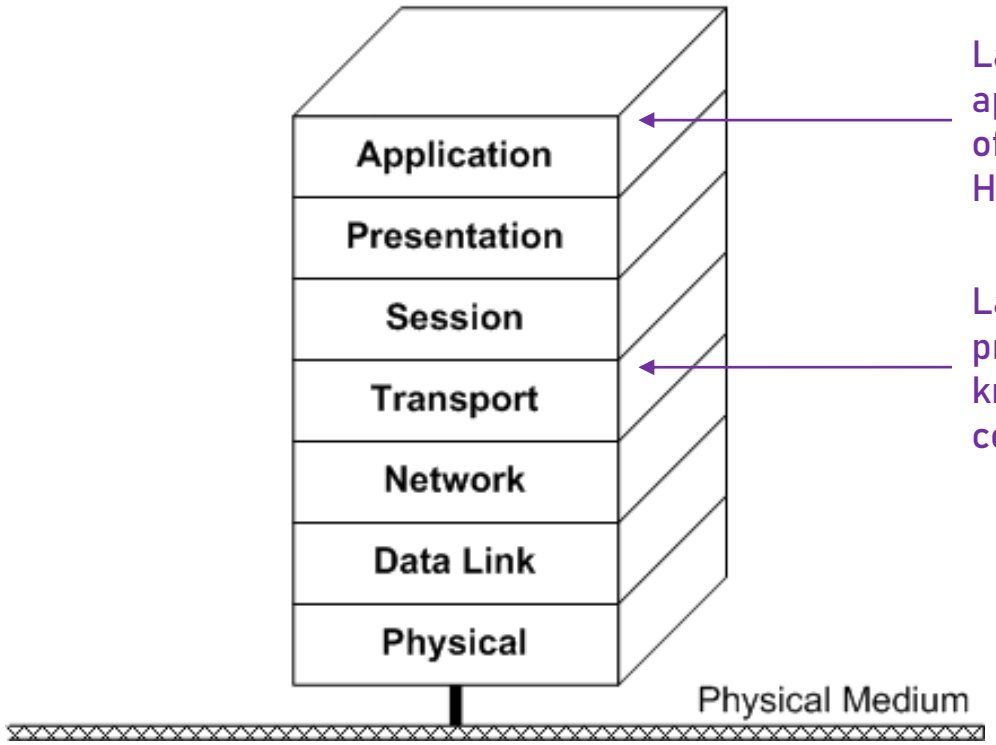
- Web traffic load balancer
- Can function as the external endpoint of the web app
- Works with:
  - VMs
  - VM Scale Sets
  - App Services
  - Kubernetes (requires some hacking…)

Application Gateway

- Similar to the Load Balancer…
- With additional features:
  - SSL Termination
  - Autoscaling
  - Zone redundancy
  - Session affinity
  - URL based routing
  - WebSocket and HTTP/2 support
  - Custom error pages
  - Header & URL rewrite
  - WAF
  - And more…

Application Gateway

- Operates at layer 7 of the OSI model

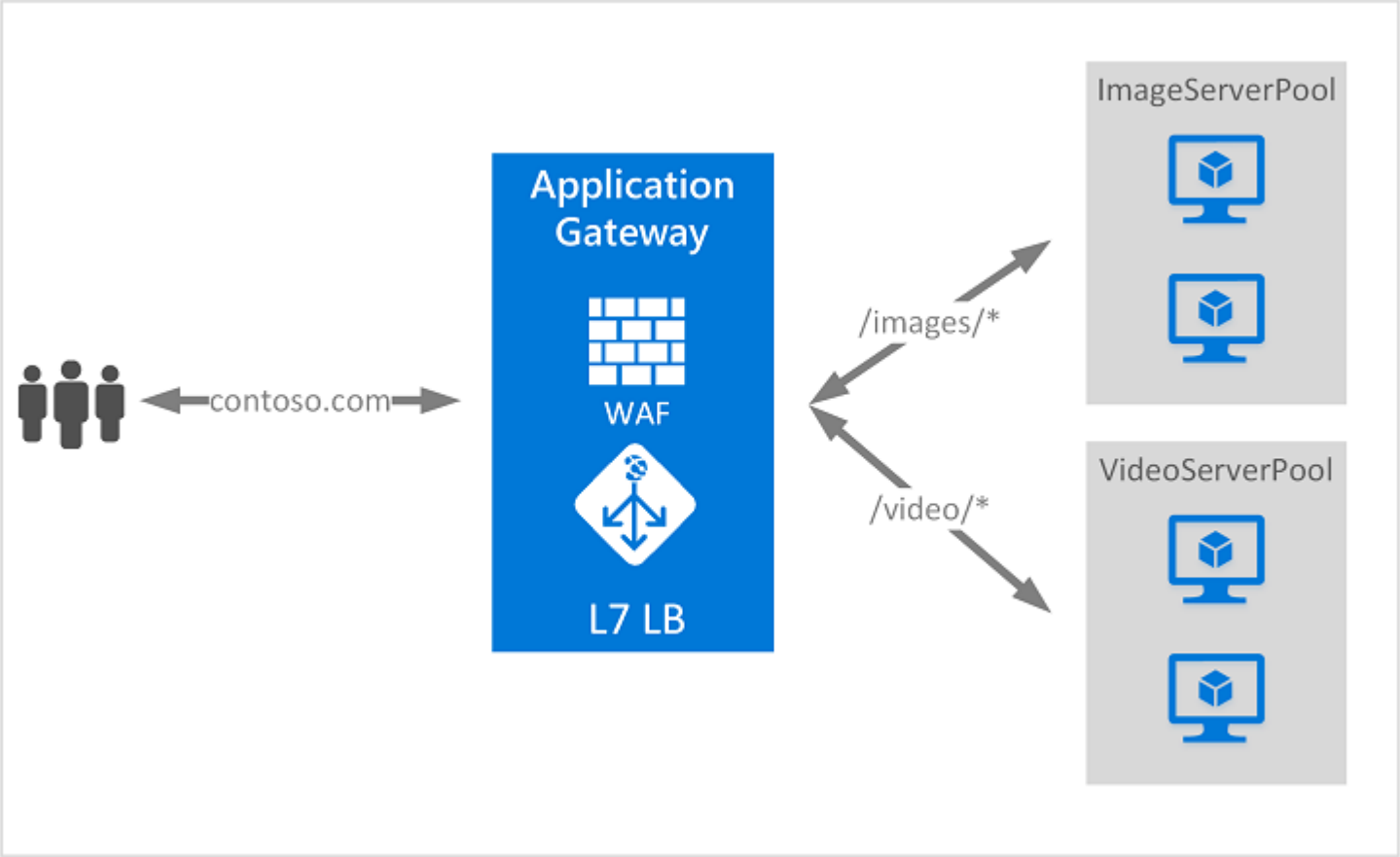


Layer 7: Interacts with the application. Can see the content of the transmission. Example: HTTP URL + path + params

Layer 4: Knows about IP, Port, protocol, TLS and more. Has no knowledge about the actual content

Application Gateway

- Operates at layer 7 of the OSI model



WAF

- Web Application Firewall
- Protects web apps against common attacks
  - ie. Cross-site scripting, SQL injection, etc.
- Protection rules based on OWASP Core Rule Set
- Updates continuously
- Works in Detection or Prevention mode

WAF

- Many organizations have their own WAF deployment
- Usually based on 3rd party products (Palo Alto, Fortinet, Imperva etc.)
- In these cases – there's no need for the WAF in the Application Gateway

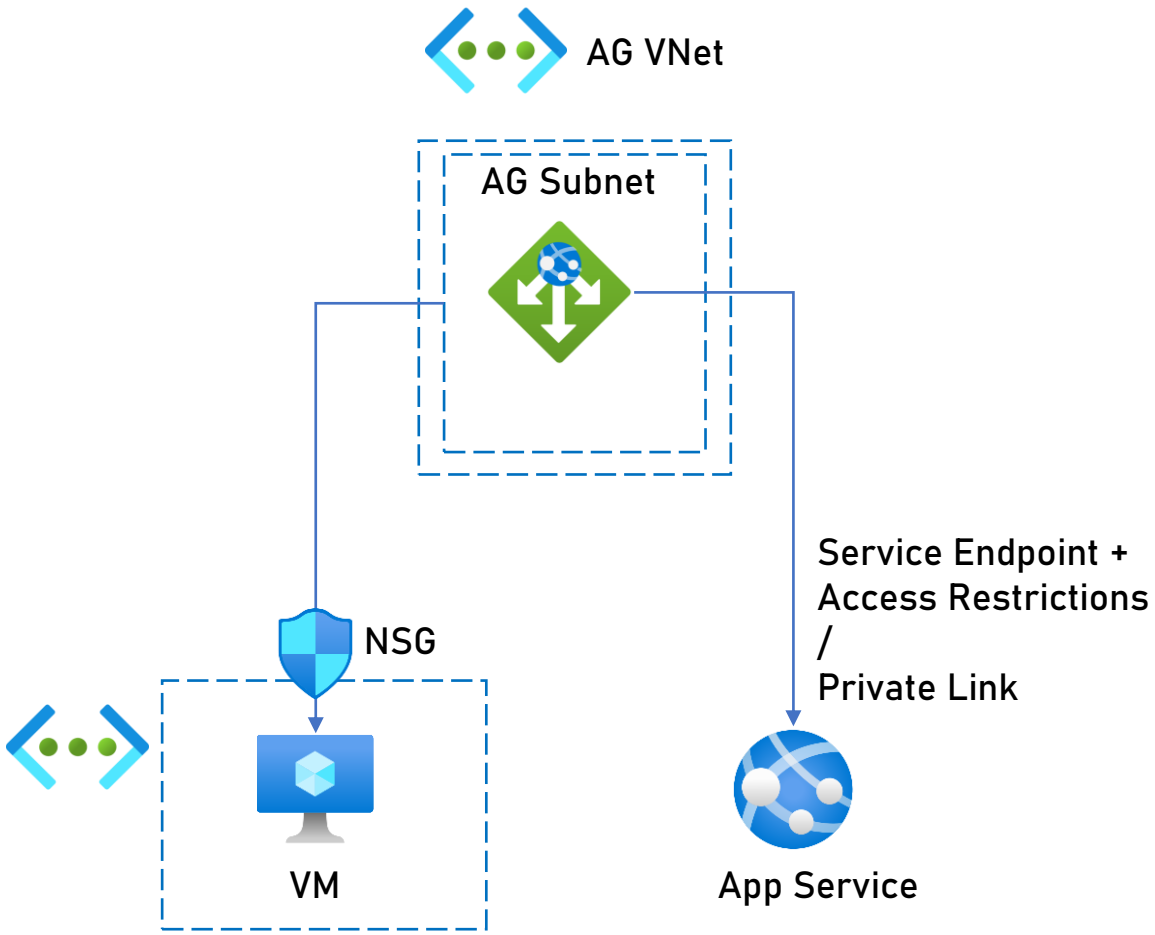
Application Gateway SKUs

- Standard_V2 – includes all the features mentioned, excluding WAF
- WAF_V2 – Includes everything (almost double the price…)

Application Gateway Networking

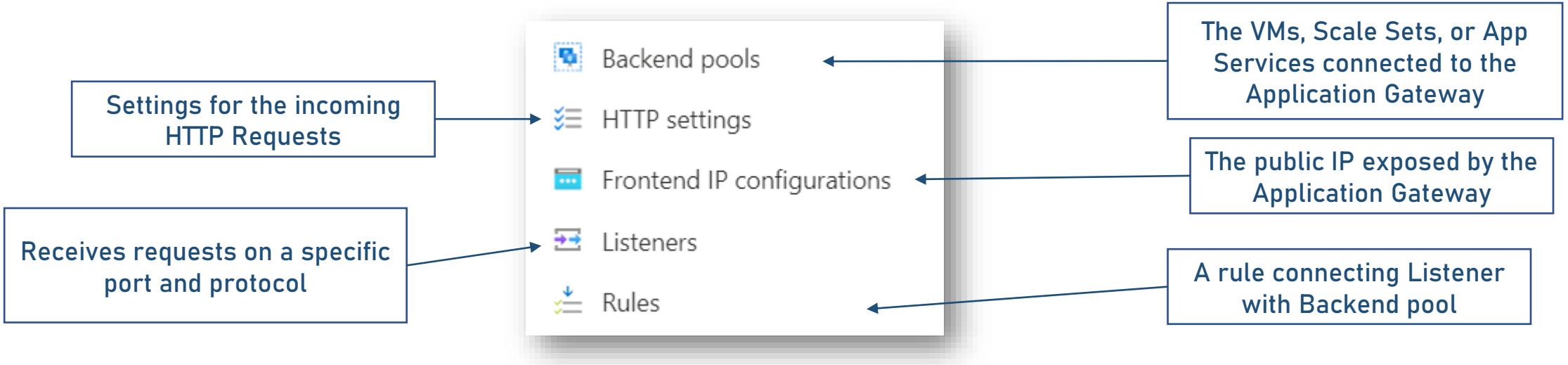
- Application Gateway is placed in its own Subnet
- Often in its own VNet
- Must make sure backend resources are:
  - Accessible from the AG Subnet
  - Not accessible from anywhere else…

Application Gateway Networking



Configuring Application Gateway

- 5 main configurations:



Application Gateway and AKS

- No built-in integration with AKS
- AKS has kind-of gateway (=services)
- There's Application Gateway Ingress Controller (AGIC) that does this
  - In preview mode, quite buggy, not recommended
- Better use 3rd party products

Application Gateway and Functions

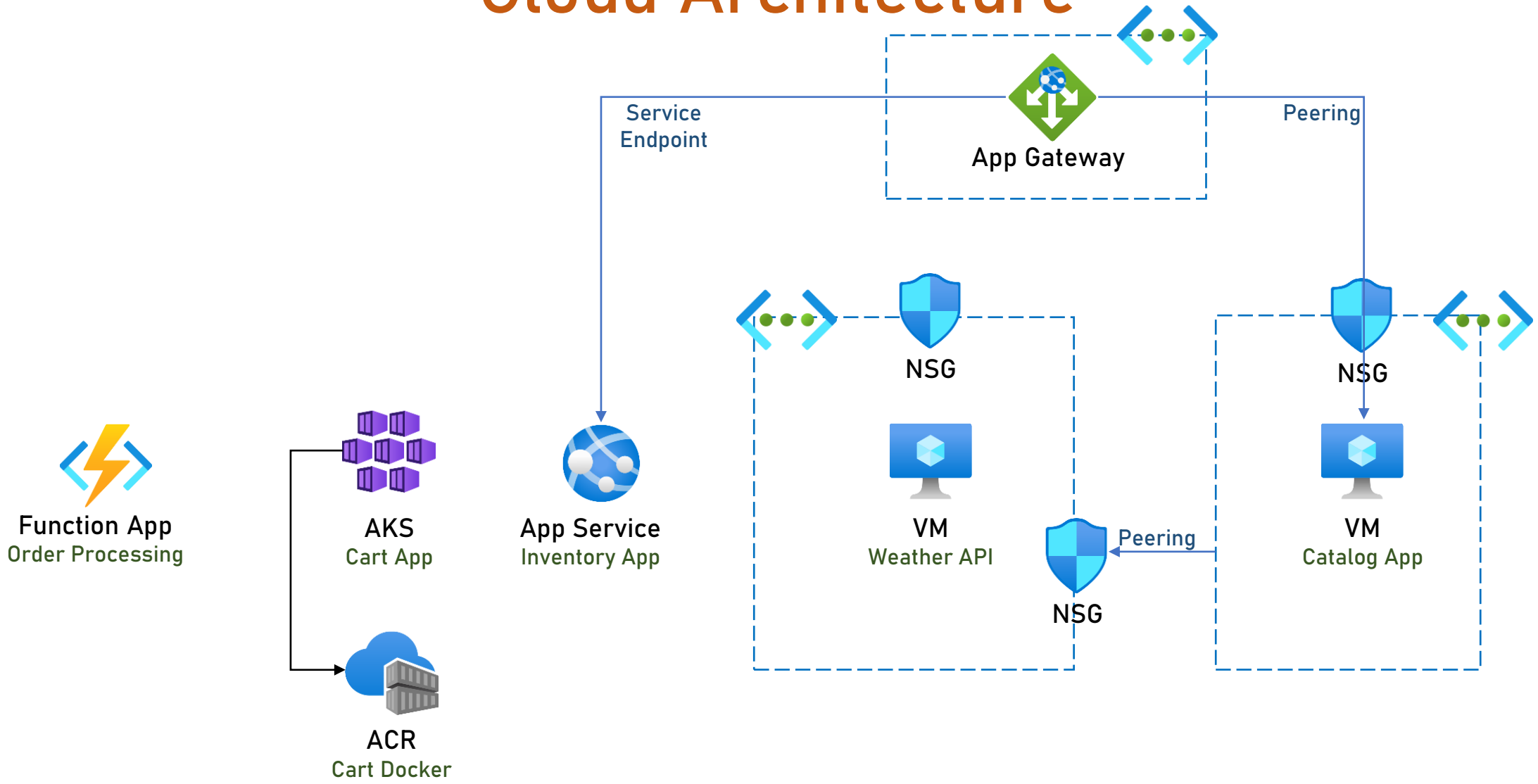
- Functions Apps are basically App Services
- They can be protected by Application Gateway the same way

  App Services are

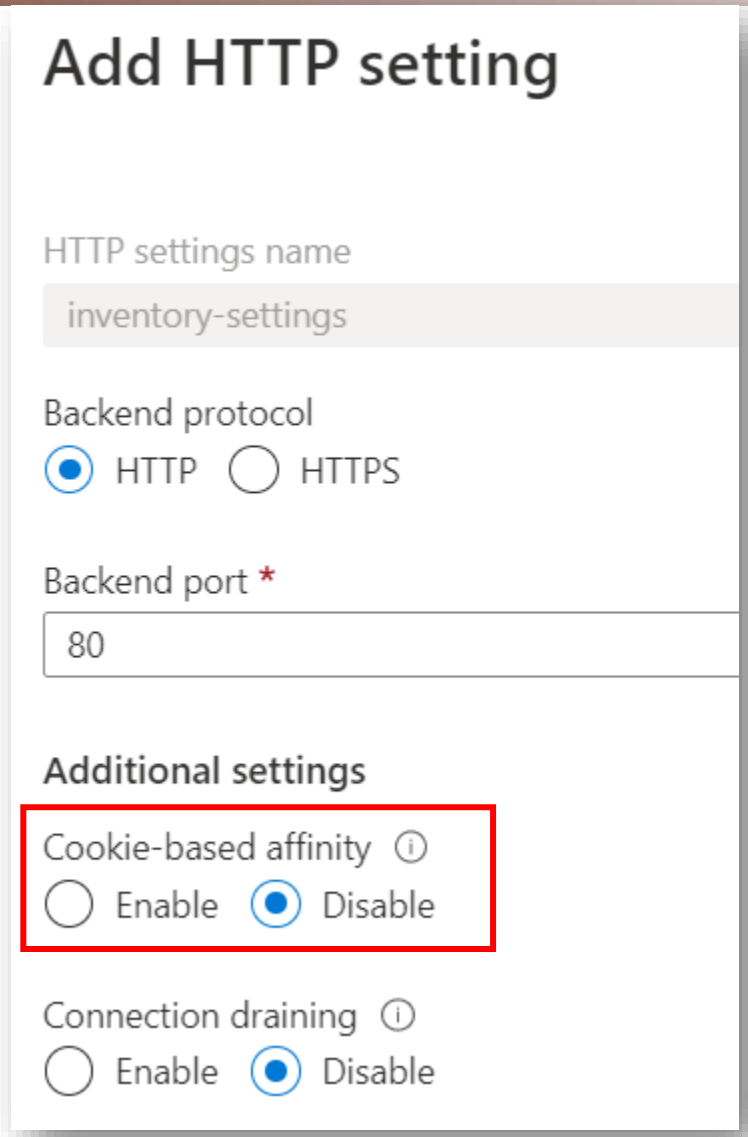
  - Configure in Backend pool
  - Configure Access Restrictions
- Our function won't be accessible from the web so no demo…

ReadIt!

Cloud Architecture



Affinity


Add HTTP setting
HTTP settings name
inventory-settings
Backend protocol
HTTP
HTTPS
Backend port *
80
Additional settings
Cookie-based affinity
Enable
Disable
Connection draining
Enable
Disable

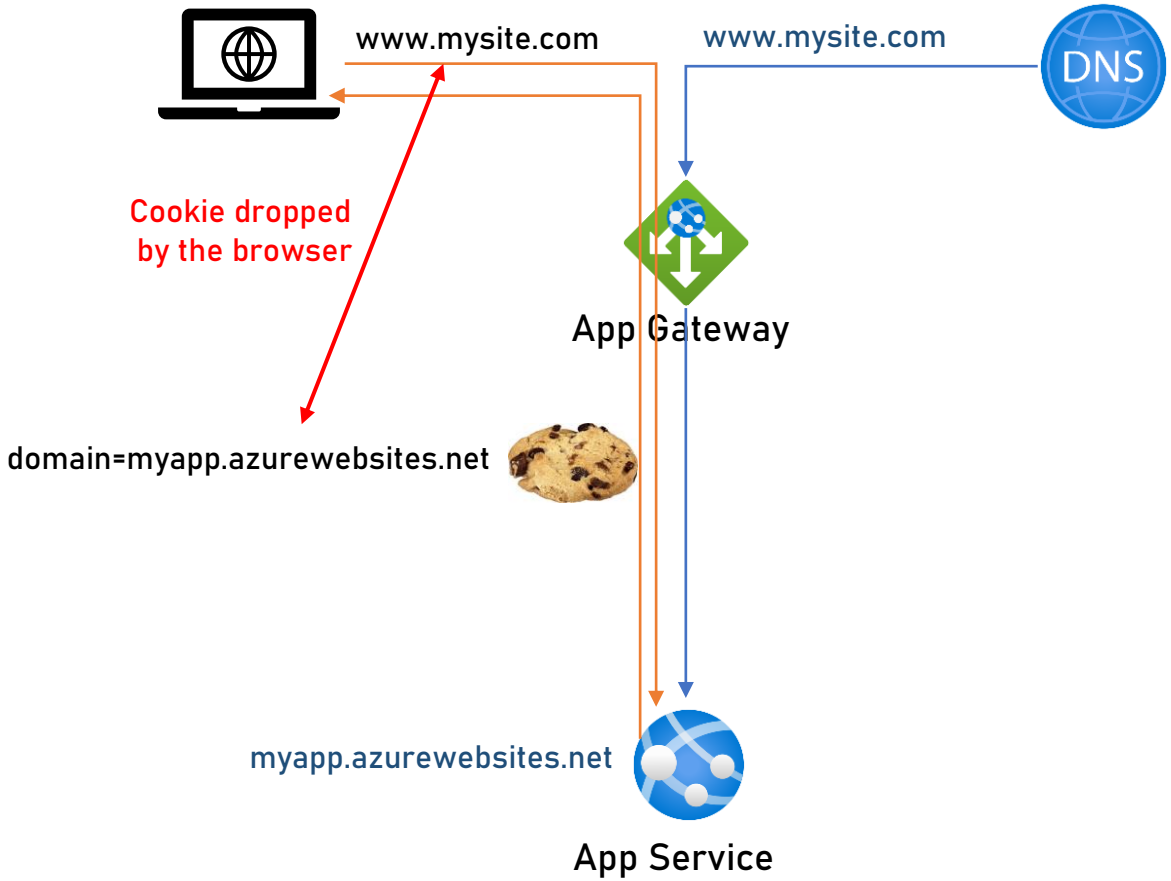
Affinity

- Makes sure user will always be directed to the same instance (VM / App Service) it began with
- Should be avoided when possible
- Usually required in Stateful apps
- Usually a sign of bad design
- Always try to design Stateless app

Application Gateway and Cookies

Super Advanced

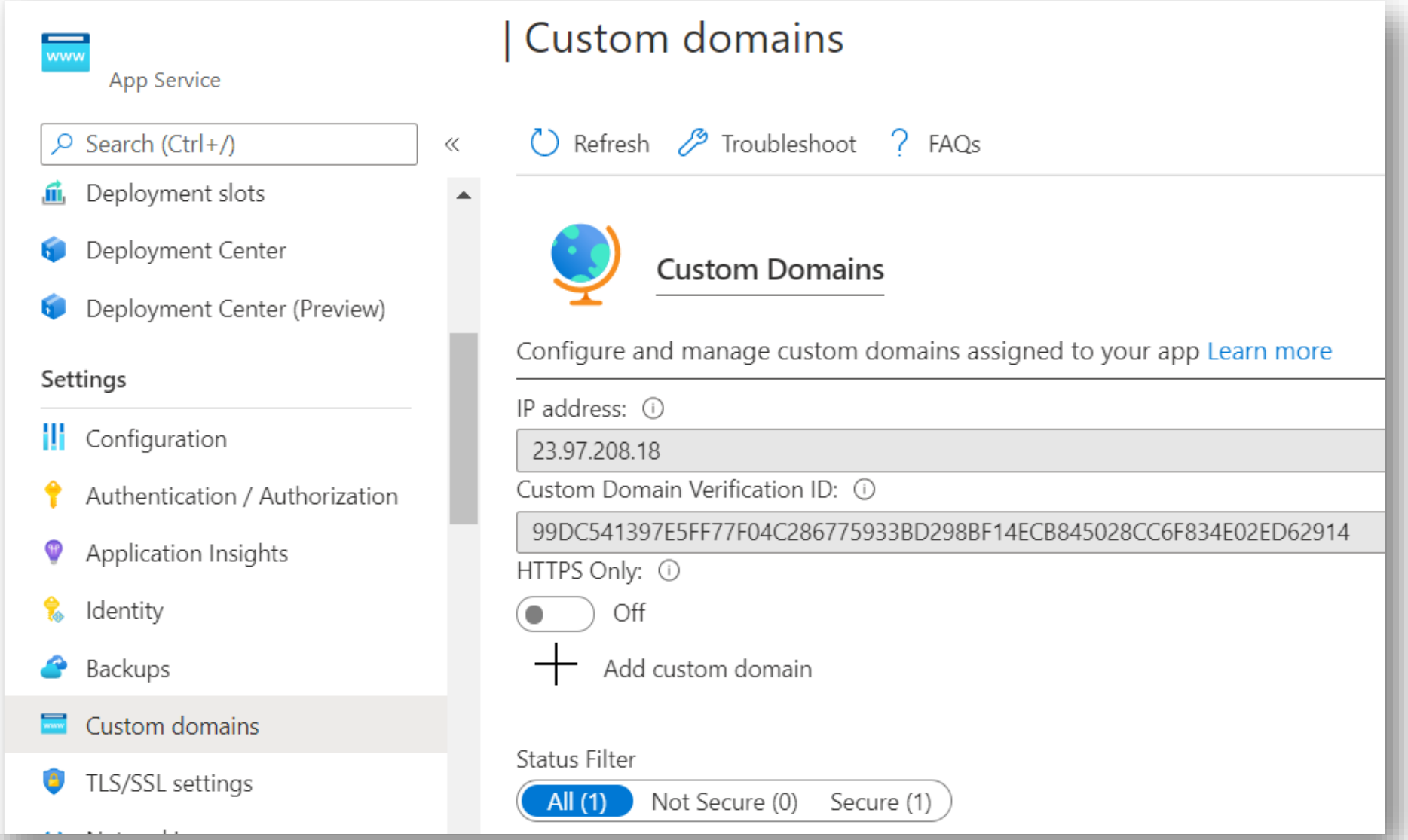
Application Gateway and Cookies



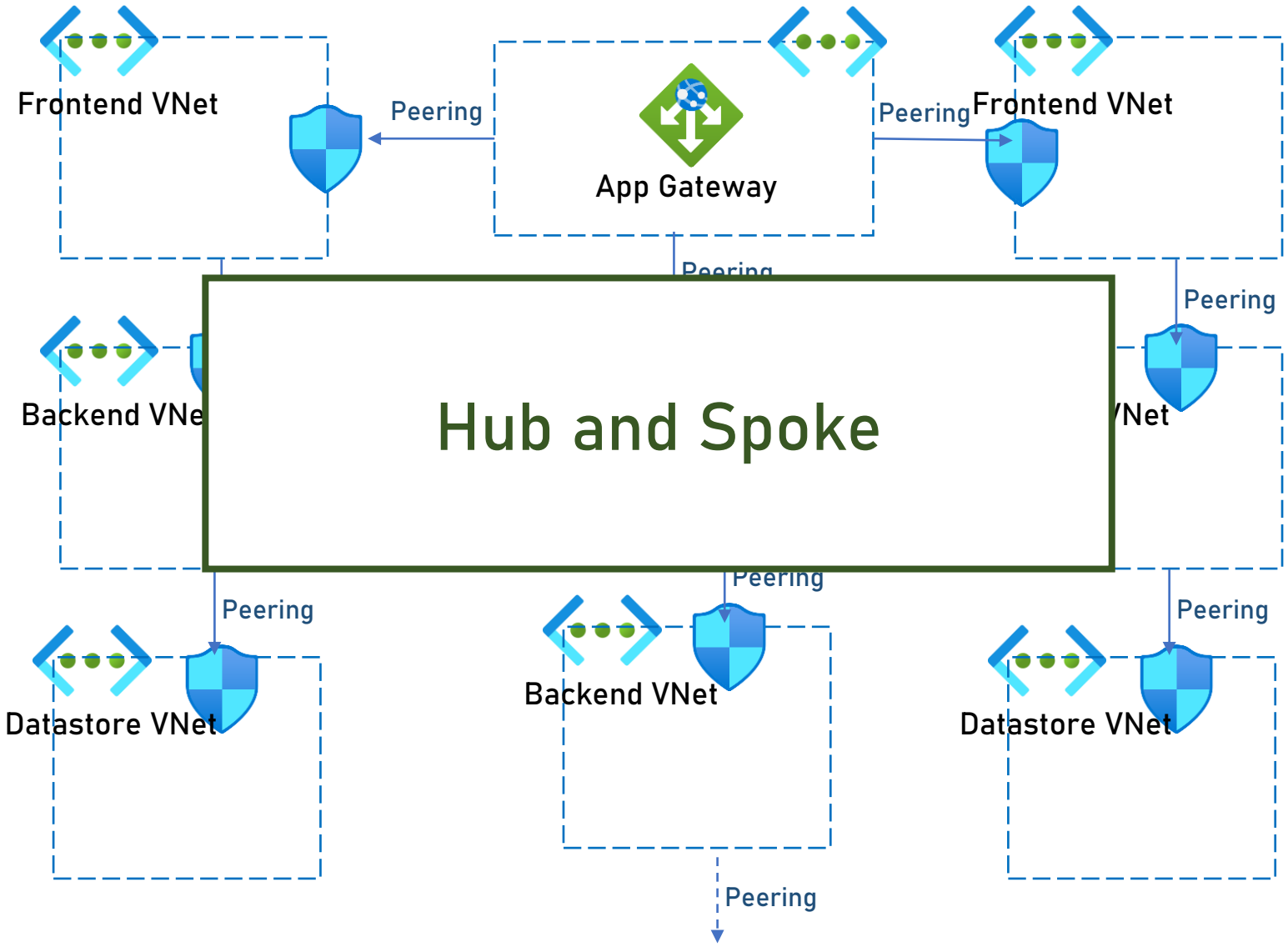
Application Gateway and Cookies

- The solution:
  - Set custom domain for the App Service to be the same one of the Application Gateway

Application Gateway and Cookies



Secure Network Design



Data in Azure

Memi Lavi
www.memilavi.com

Data in Azure

- Azure provides many data solutions as cloud services
- Relational databases, NoSQL databases, object stores
- Fully managed services
- Can be part of Azure app or completely independent
- Various pricing models
- Always better than unmanaged solutions

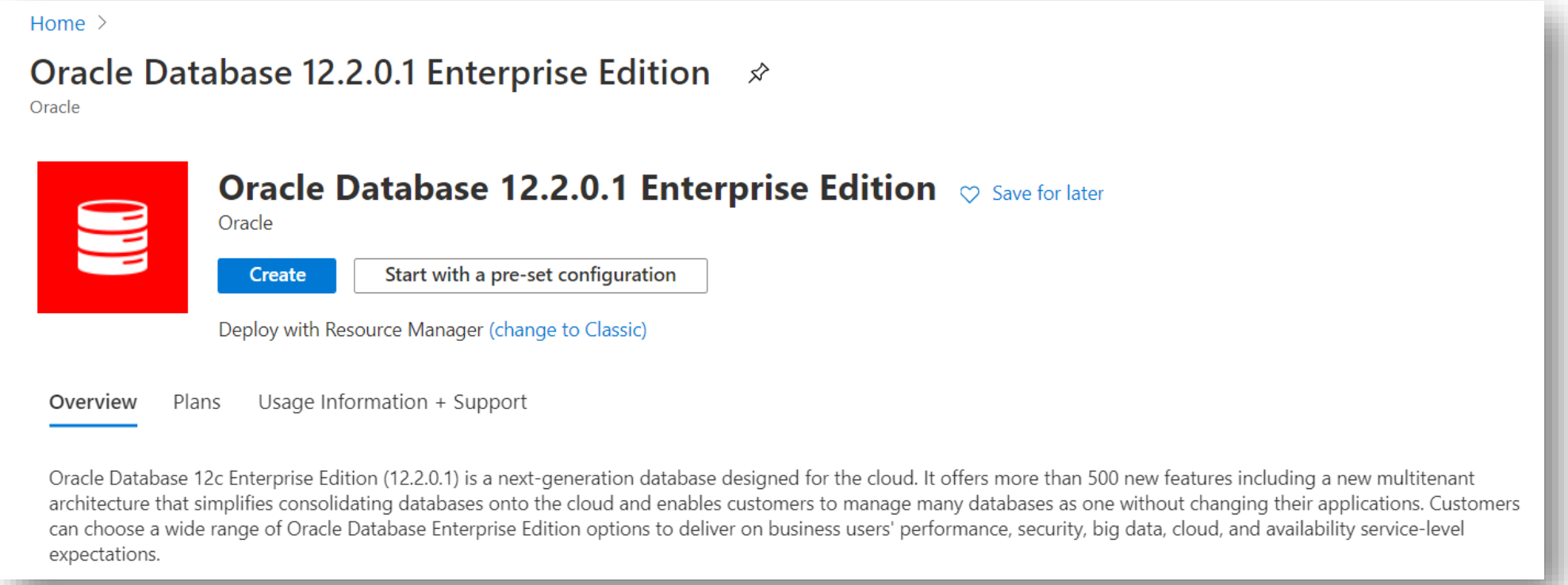
Major Database Features

- What to look for when selecting a database?

Security	Network isolation, Encryption
Backup	Backup types, Retention Period
Availability	SLA, Replication, DR

Database on VM

- Azure VM can be setup with database software
- There are ready-made VMs in the marketplace



Database on VM

- Pros of Database on VM:
  - Full flexibility
  - Full control

Database on VM

- Cons of Database on VM:
  - You have to take care of everything:
    - SLA
    - Updates
    - Availability
    - Security
    - Backups
    - And more…

Database on VM

- In this section we'll discuss only managed databases

Azure SQL

- Managed SQL Server on Azure
- Works like any other SQL Server using the same tools
- Great compatibility with on-prem SQL Server
  - Depends on the exact Azure SQL Flavor
- Offers built-in security, backups, availability and more
- Flexible pricing models

Azure SQL Flavors

Azure SQL Database

Elastic Pool

Managed Instance

Azure SQL Database

- Managed SQL Server on Azure
- Single database on a single server
- Automatic backups, updates, scaling
- Good compatibility with on-prem SQL Server
  - Not all features are supported

Azure SQL Database

- Security:
  - IP firewall rules
  - Service Endpoints
  - SQL & Azure AD Authentication
  - Secure communication (TLS)
  - Data encrypted by default (TDE)

Azure SQL Database

- Backup:

Full	→	Every week
Differential	→	Every 12-24 hrs
Transaction Log	→	Every 5-10 mins

Azure SQL Database

- Retention Period:
  - Regular backup: 7-35 days (default is 7)
  - Long term backup: up to 10 years

Azure SQL Database

- Availability:
  - Backup is stored in a geo-redundant storage
  - Active geo-replication
  - SLA: 99.9% - 99.995%, depends on tier and redundancy

Azure SQL Database

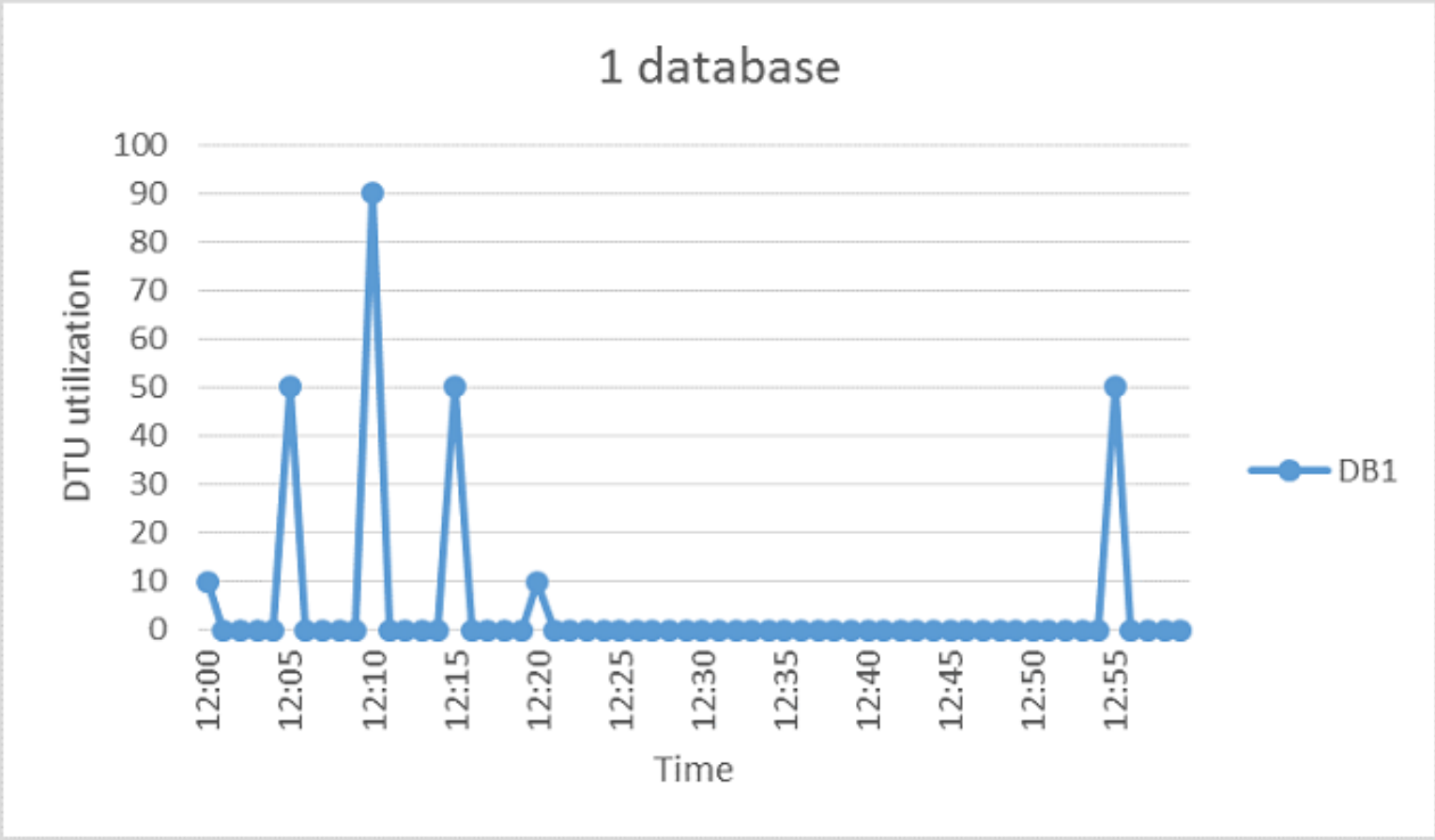
- Compute Tiers:

Provisioned	Serverless
• Pay for allocated resources regardless of actual use • Can be reserved	• Pay for actual use – vCore + RAM / second • Automatically paused when inactive (pay just for storage) • Slight delay when warming up • Can't be reserved

Elastic Pool

- Based on Azure SQL
- Allows storing multiple databases on single server
- Great for databases with low average utilization and infrequent spikes

Elastic Pool



Elastic Pool

Elastic Pool

- Cost effective
- Purchase the compute resources you need, not the database

Managed Instance

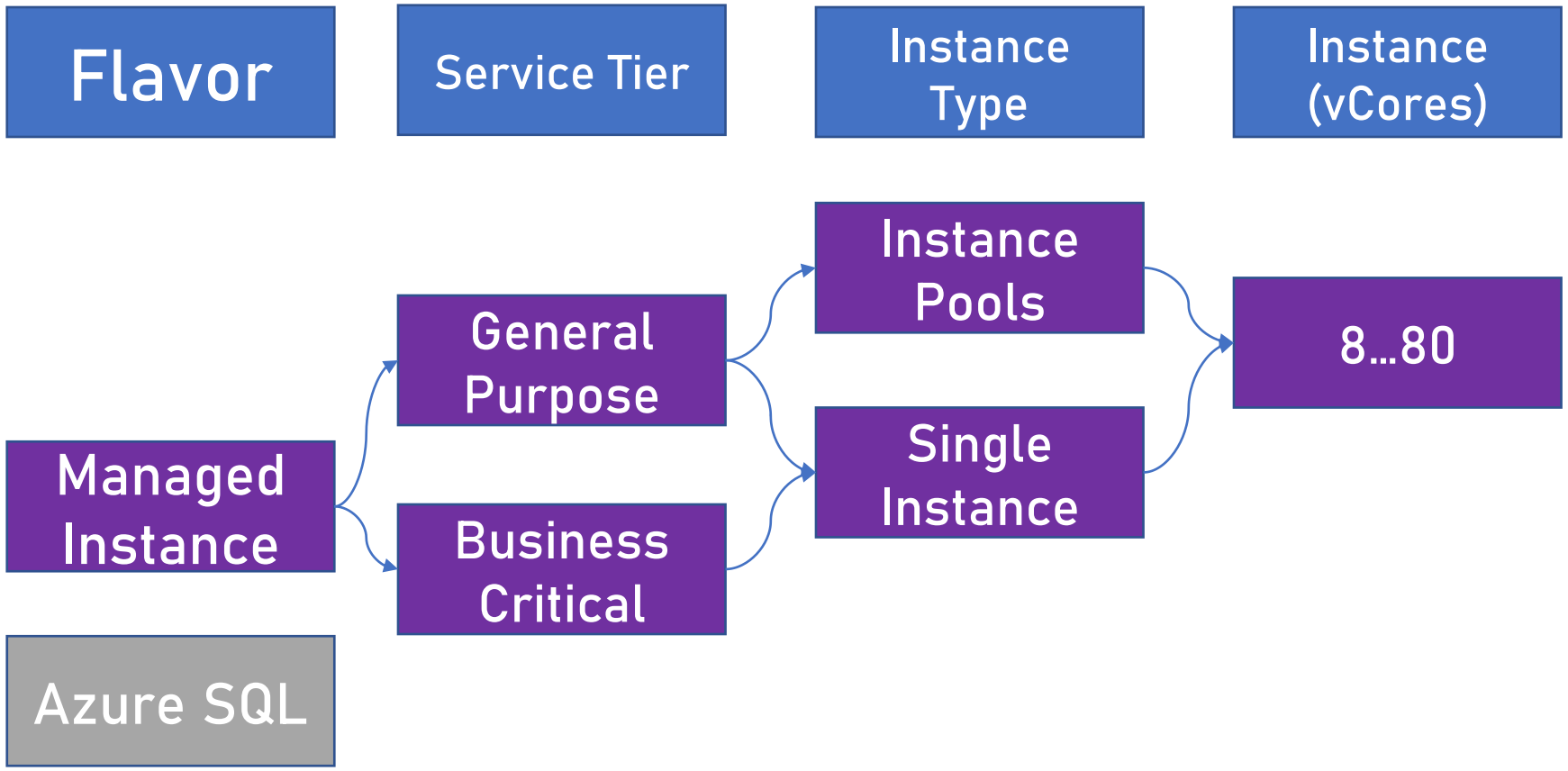
- Closer to the on-prem SQL Server
- Near 100% compatible with on-prem SQL
- Can be deployed to VNet
- Business model close to on-prem one

Managed Instance

- Main differences:
  - No active geo-replication
  - SLA: 99.99%
  - Supports built-in functions
  - Runs CLR code
  - No auto scaling & tuning
  - No availability zone
  - No serverless tier
  - No Hyperscale

Azure SQL Pricing

Quite complicated…


Flavor
Service Tier
Instance Type
Instance (vCores)
Instance Pools
General Purpose
8…80
Single Instance
Managed Instance
Business Critical
Azure SQL

Azure SQL Managed Instance

REGION: West India

TIER: Managed Instance

BACKUP STORAGE TIER: RA-GRS

SERVICE TIER: General Purpose

INSTANCE TYPE: Single Instance

GENERATION: Gen 5

INSTANCE: 8 vCore

Savings Options

Save up to 73% on pay as you go prices with 1 year or 3 year reserved options.

Compute

- (●) Pay as you go
- ( ) 1 year reserved
- ( ) 3 year reserved

$977.84
Average per month
($0.00 charged upfront)

SQL License

- (●) Pay as you go
- ( ) Azure Hybrid Benefit

$583.80
Average per month
($0.00 charged upfront)

= $1,561.65
Average per month
($0.00 charged upfront)

1 Instances × 730 Hours

Azure SQL Managed Instance

REGION: West India

TIER: Managed Instance

BACKUP STORAGE TIER: RA-GRS

SERVICE TIER: Business Critical

INSTANCE TYPE: Single Instance

GENERATION: Gen 5

INSTANCE: 24 vCore

Savings Options

Save up to 73% on pay as you go prices with 1 year or 3 year reserved options.

Compute

- (●) Pay as you go
- ( ) 1 year reserved
- ( ) 3 year reserved

$5,867.08
Average per month
($0.00 charged upfront)

SQL License

- (●) Pay as you go
- ( ) Azure Hybrid Benefit

$6,570.00
Average per month
($0.00 charged upfront)

= $12,437.08
Average per month
($0.00 charged upfront)

Azure SQL Managed Instance

REGION:
West India

TIER:
Managed Instance

BACKUP STORAGE TIER:
RA-GRS

SERVICE TIER:
Business Critical

INSTANCE TYPE:
Single Instance

GENERATION:
Gen 5

INSTANCE:
24 vCore

Savings Options

Save up to 73% on pay as you go prices with 1 year or 3 year reserved options.

Compute

- ○ Pay as you go
- ○ 1 year reserved
- ◉ 3 year reserved

COMPUTE PAYMENT OPTIONS:
Upfront

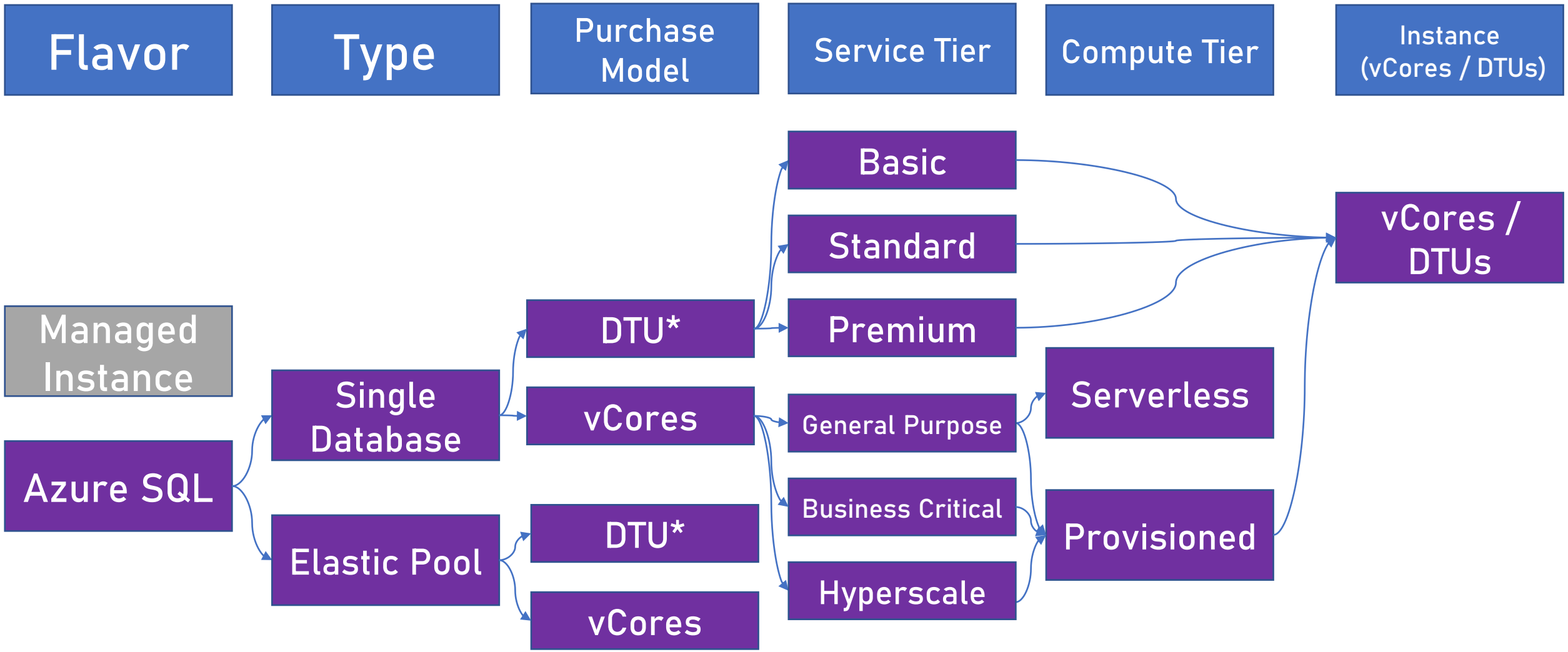
$2,639.91
Average per month
($95,036.89 charged upfront)

SQL License

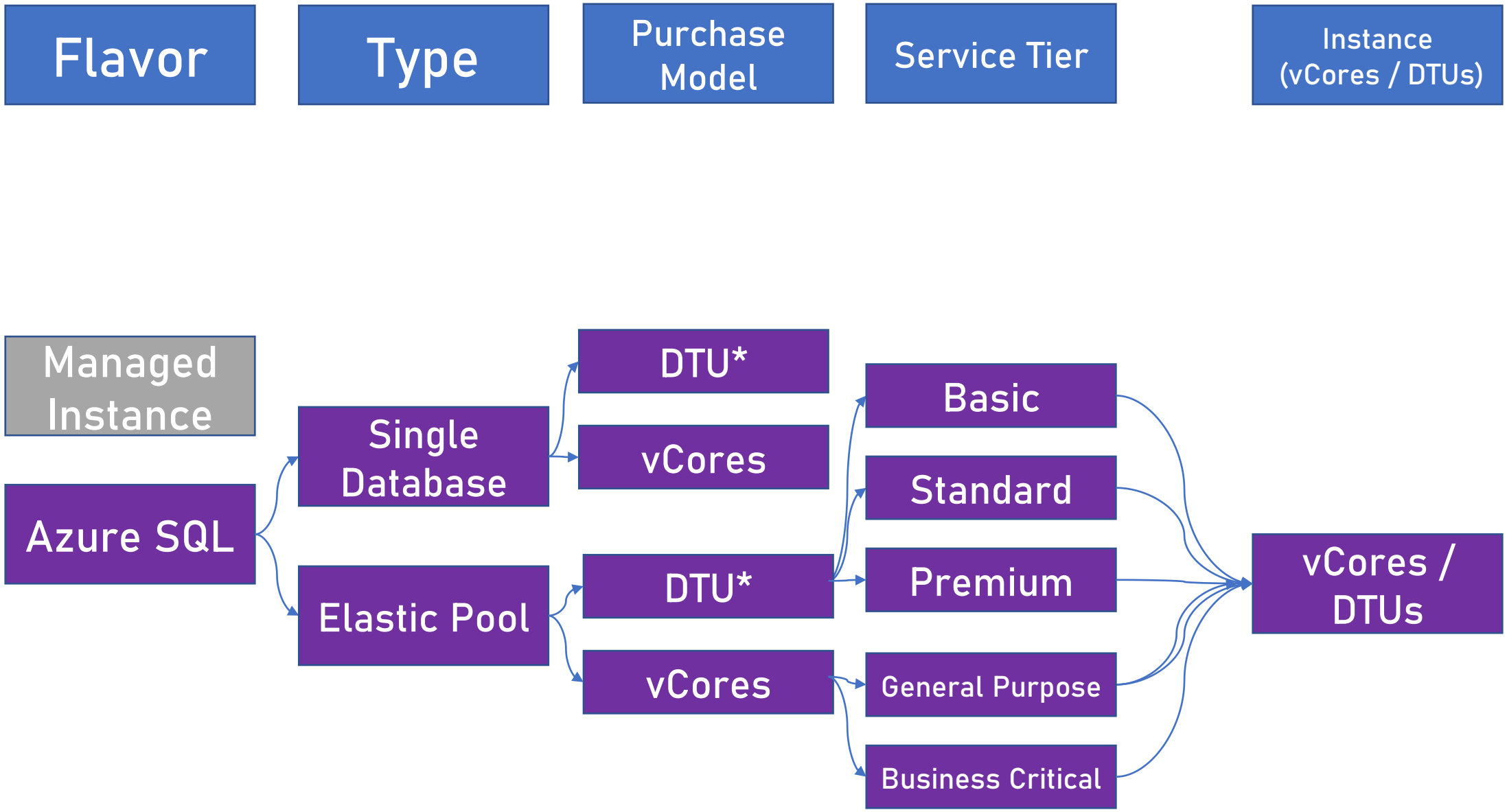
- ◉ Pay as you go
- ○ Azure Hybrid Benefit

$6,570.00
Average per month
($0.00 charged upfront)

= $9,209.91
Average per month
($95,036.89 charged upfront)



1 vCore =~ 100 DTU



1 vCore =~ 100 DTU

Azure SQL Database

REGION:
East US

TYPE:
Single Database

BACKUP STORAGE TIER:
RA-GRS

PURCHASE MODEL:
DTU

SERVICE TIER:
Standard

PERFORMANCE LEVEL:
S1: 20 DTUs, 250 GB included storage per DB, $0.0403/hour

1
Databases

×

730 Hours

= $29.43

Azure SQL Database

REGION: East US

TYPE: Single Database

BACKUP STORAGE TIER: RA-GRS

PURCHASE MODEL: vCore

SERVICE TIER: Business Critical

HARDWARE TYPE: Gen 5

INSTANCE: 12 vCore

Compute

1 Instances × 730 Hours

Savings Options

Save up to 73% on pay as you go prices with 1 year or 3 year reserved options.

Compute

- (●) Pay as you go
- ( ) 1 year reserved
- ( ) 3 year reserved

$2,666.85
Average per month
($0.00 charged upfront)

SQL License

- (●) Pay as you go
- ( ) Azure Hybrid Benefit

$3,285.00
Average per month
($0.00 charged upfront)

= $5,951.85
Average per month
($0.00 charged upfront)

Azure SQL Database

REGION:	TYPE:	BACKUP STORAGE TIER:	PURCHASE MODEL:
East US	Single Database	RA-GRS	vCore

SERVICE TIER:	COMPUTE TIER:	HARDWARE TYPE:
General Purpose	Serverless	Gen 5

Billed vCores

Maximum vCores:	Minimum vCores:
8	2

4	12	2678400
CPU Used (vCores)	Memory used (GB)	Duration (in seconds, max 2,678,400 seconds (744 hours))

Minimum memory	6 GB
Maximum memory	24 GB
Billed vCores ⓘ	4

Highly inaccurate

= $1,552.75

Which Azure SQL to Choose?

Are you migrating an on-prem SQL? → Managed Instance

Do you need multiple, mostly low-utilization DBs? → Elastic Pool

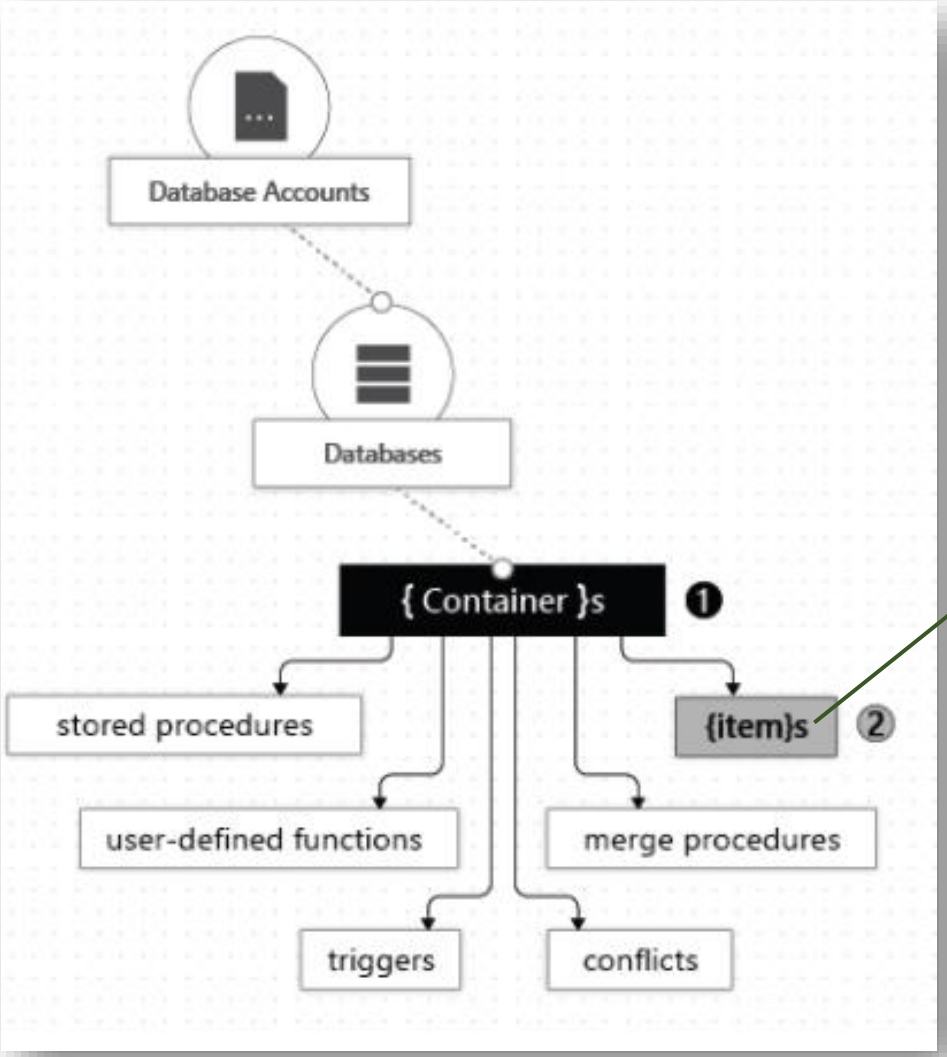
All other cases → Azure SQL

Cosmos DB

- Fully managed NoSQL database
- Amazing performance - <10ms for 99% of operations
- Globally distributed
- Fully automatic management – updates, scaling, fixes etc.
- Multiple APIS:
  - SQL, Mongo, Gremlin, Azure Table, Cassandra (per account)

Cosmos DB

- Hierarchical:



JSON Document

Cosmos DB Availability

- Can be distributed across many regions (configurable)
- API automatically picks the closest one
- When using write replication SLA is 99.999% (!)
- Managed automatically, no code changes required

Cosmos DB Backup

- Full backup every 1-24 hours (default is 4)
- Retention period 20-30 days (default is 30)

Cosmos DB Security

- IP firewall rules
- Service Endpoints
- Private Endpoints
- Azure AD Authentication
- Secure communication (TLS)
- Data encrypted by default

Cosmos DB Partitions

- Data items are divided to partitions
- Logical group of items based on a specific property
- Example: In a cars database, the Model can be a partition property

Cosmos DB Partitions

- Partitions are the basic scale unit in Cosmos DB
- Distribution and scale are per partitions
- Make sure items are divided as evenly as possible
- It's extremely important to select the right partition property
- Cannot be modified

Recording of L7S5 from the Architecture course

Cosmos DB Consistency Levels

- Traditionally:
  - Relational DB – Strong consistency: Call returns only after successful commit in all replicas (High availability)
  - NoSQL DB – Eventual consistency: Call returns immediately, commit in replicas happens later (Low latency)

High Availability ≠ Low Latency

Cosmos DB Consistency Levels

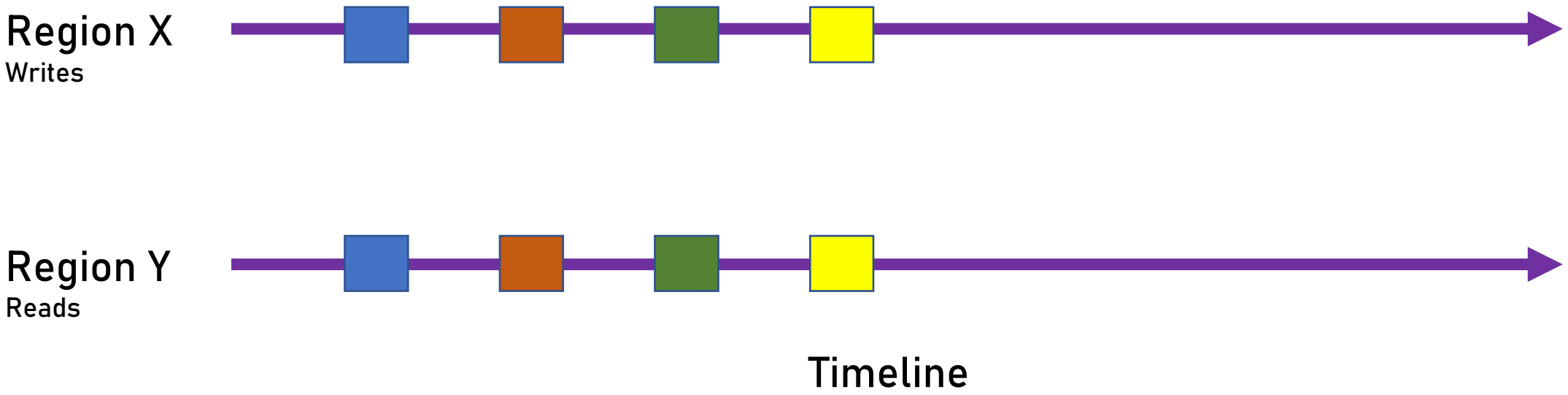
- Cosmos DB offer five consistency levels:
  - Strong (<= As in regular relational DB)
  - Bounded Staleness
  - Session
  - Consistent Prefix
  - Eventual (<= As in regular NoSQL DB)

Cosmos DB Consistency Levels

- The basic question with consistency is:
  - If region X updates an item, and region Y reads this item, which version will it get?

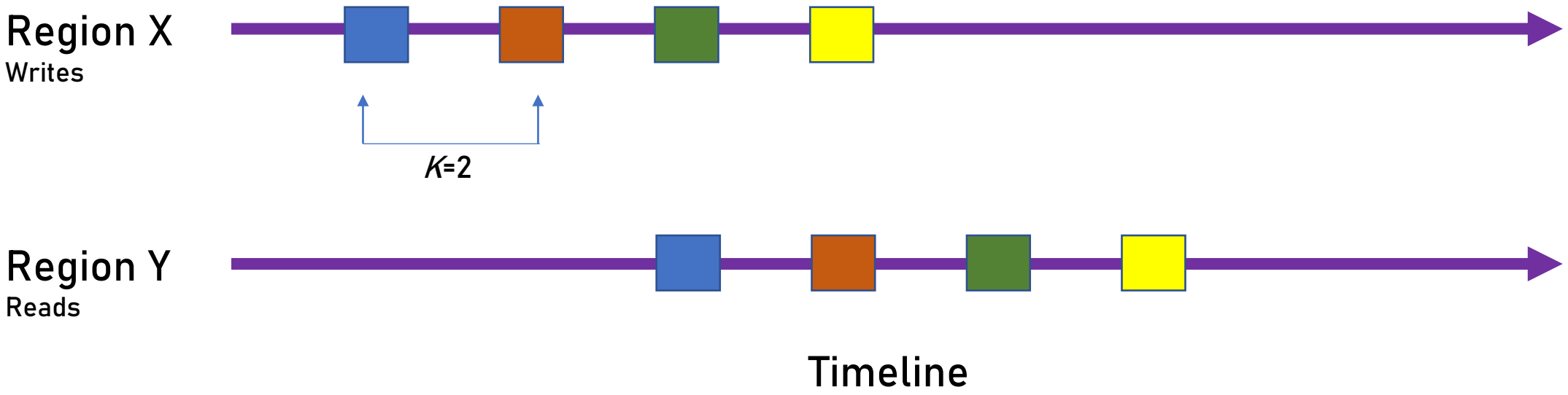
Strong

- Region Y will get the last version of the item updated in region X
- Used for mission critical data



Bounded Staleness

- Region Y will lag behind region X by *K* versions or *T* time
- Keeps the order of the versions
- Used for low write latency and when order is important

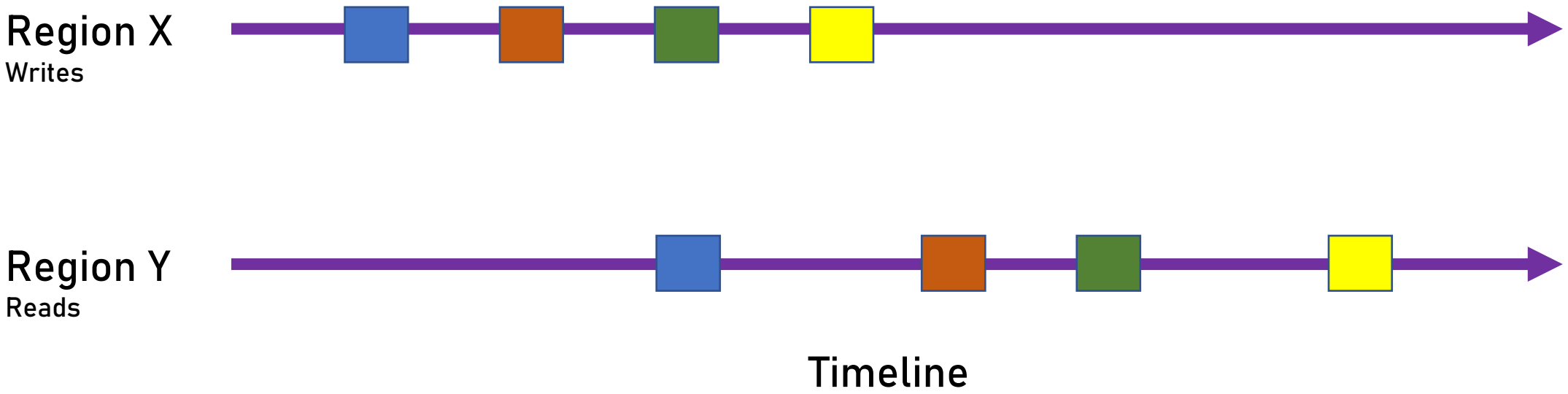


Session

- In a client session – Strong consistency
- Other clients – Consistent Prefix (sometimes Eventual)

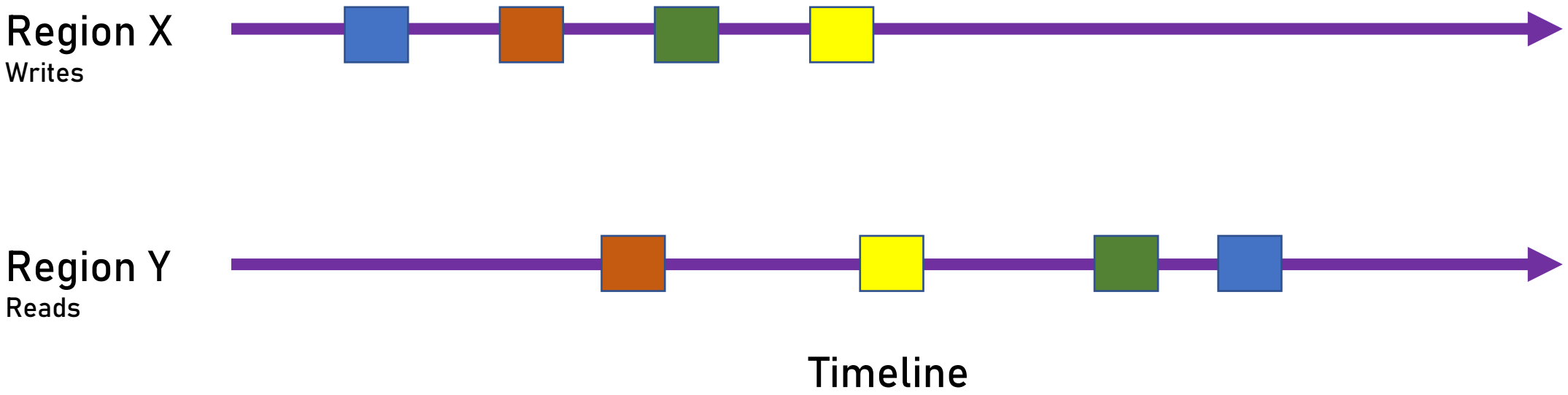
Consistent Prefix

- Keeps the order of the versions
- No guarantee of the lag size (as opposed to Bounded Context)
- Used for low write latency and when reads are infrequent



Eventual

- No order guarantee
- No guarantee of the lag size (as opposed to Bounded Context)
- Used for count of Retweets, Likes, etc.



Cosmos DB Consistency Levels

- Configured at the account level
- Can be relaxed on the request level

Cosmos Pricing

- Based on RU/s
  - Request Unit per Second
- 1 RU = Read item of size 1KB
  - Read = Get the item by its ID, not by query

Cosmos Pricing

- 1 RU/s = Read 1 item of 1KB in 1 sec
- 400 RU/s = Read 400 items of 1KB in 1 sec
- Update, delete, insert, query – more than 1 RU
- You can see the actual RU consumed in the response header of the results

Cosmos Pricing

- Pricing based on:
  - Operations type: Provisioned, Auto Scale, Serverless
  - Write Regions
  - No. of provisioned RU/s

Cosmos Pricing

- Database Operations:
  - Provisioned – Predefined number of RU/s, can be changed manually later. Offers reserved capacity up to 65% discount
  - Auto Scale – Set the maximum RU/s, Cosmos scales up to this number. Good for unpredictable loads
  - Serverless – Pay for what you use. In Preview, no SLA

Azure Cosmos DB

DATABASE OPERATIONS:

Standard provisioned throughput (manual)

WRITE REGIONS:

Single Region Write (Single-Master)

Savings Options

Save up to 65% on pay as you go prices with 1-year or 3-year reserved capacity for Azure Cosmos DB.

- (●) Pay as you go
- ( ) 1 year reserved capacity
- ( ) 3 year reserved capacity

$23.36
Average per month
($0.00 charged upfront)

Request units per second (RU/s)

4
X100 RU/S

×

730 Hours

ENABLE AVAILABILITY ZONES

Region:

East US

	4	×	730	×	$0.008	=	$23.36
	x100 RU/s		Hours		Per hour		

Azure Cosmos DB

DATABASE OPERATIONS:

Standard provisioned throughput (manual)

WRITE REGIONS:

Multiple Region Write (Multi-Master)

Savings Options

Save up to 65% on pay as you go prices with 1-year or 3-year reserved capacity for Azure Cosmos DB.

- (●) Pay as you go
- ( ) 1 year reserved capacity
- ( ) 3 year reserved capacity

$584.00
Average per month
($0.00 charged upfront)

Request units per second (RU/s)

50 × 730 Hours

X100 RU/S

Region:

East US

50	×	730	×	$0.016	=	$584.00
x100 RU/s		Hours		Per hour		

Azure Cosmos DB

DATABASE OPERATIONS:

Autoscale provisioned throughput

WRITE REGIONS:

Single Region Write (Single-Master)

Savings Options

Pay as you go

$876.00
Average per month
($0.00 charged upfront)

Maximum Request Units Per Second (RU/s)

10
X1,000 RU/S

×

730 Hours

×

100
AVERAGE % UTILIZATION

ENABLE AVAILABILITY ZONES

Region:

East US

10	×	730	×	$0.120	×	100%	=	$876.00
x1,000 RU/s		Hours		Per hour		Average Utilization		

Azure MySQL

- Managed MySQL on Azure
- Works like any other MySQL database using the same tools
- Great compatibility with on-prem MySQL database
- Offers built-in security, backups, availability and more

Azure MySQL

- Security:
  - IP firewall rules
  - Service Endpoints
  - Private Endpoints
  - Regular & Azure AD Authentication
  - Secure communication (TLS)
  - Data encrypted by default

Azure MySQL

- Backup:
  - Depends on Service Tier:
    - Basic – Full backup: daily
    - General Purpose up to 4GB:
      - Full backup: once a week
      - Differential backup: twice a day
      - Transaction log backup: every 5 minutes

Azure MySQL

- Backup:
  - Depends on Service Tier:
    - General Purpose up to 16GB:
      - Full backup: Once created
      - Differential backup: once a day
      - Transaction log backup: every 5 minutes

Azure MySQL

- Retention Period:
  - 7-35 days (default is 7)
  - No native long term retention support

Azure MySQL

- Availability:
  - Backup is stored in a geo-redundant storage
    - In General Purpose and Memory Optimized tiers
  - SLA: 99.99%

Azure MySQL Pricing

- Pricing based on:
  - Tier:
    - Basic – Require light compute and I/O performance (ie. dev)
    - General Purpose – Most business workloads
    - Memory Optimized – Require in-memory performance
  - Compute (no. of vCores)

Azure MySQL Pricing

- Flexible Server deployment – currently in preview, not recommended
- Reservations exist

Azure Database for MySQL

REGION: West Europe

DEPLOYMENT OPTION: Single Server

TIER: Basic

COMPUTE: Gen 5, 1 vCore, $0.0398/hour

Savings Options

Save up to 51% on pay as you go prices with the 1 year reserved option.

1 year reserved option is not available for your instance selection.

3 year reserved option is not available for your instance selection.

- (●) Pay as you go
- ( ) 1 year reserved
- ( ) 3 year reserved

$29.05
Average per month
($0.00 charged upfront)

1 Servers × 730 Hours = $29.05 Average per month

Azure Database for MySQL

REGION: West Europe

DEPLOYMENT OPTION: Single Server

TIER: General Purpose

COMPUTE: Gen 5, 4 vCore, $0.4168/hour

Savings Options

Save up to 51% on pay as you go prices with the 1 year reserved option.

- (●) Pay as you go
- ( ) 1 year reserved (~35% savings)
- ( ) 3 year reserved (~53% savings)

$304.26
Average per month
($0.00 charged upfront)

1 Servers × 730 Hours

= $304.26
Average per month
($0.00 charged upfront)

Azure PostgreSQL

- Managed PostgreSQL on Azure
- Works like any other PostgreSQL database using the same tools
- Great compatibility with on-prem PostgreSQL database
- Includes Hyperscale deployment
- Offers built-in security, backups, availability and more

Azure PostgreSQL

- Security:
  - IP firewall rules
  - Service Endpoints
  - Private Endpoints
  - Regular & Azure AD Authentication
  - Secure communication (TLS)
  - Data encrypted by default

Azure PostgreSQL

- Backup:
  - Depends on storage size:
    - up to 4GB:
      - Full backup: once a week
      - Differential backup: twice a day
      - Transaction log backup: every 5 minutes

Azure PostgreSQL

- Backup:
  - Depends on storage size:
    - up to 16GB:
      - Full backup: Once created
      - Differential backup: thrice a day
      - Transaction log backup: every 5 minutes

Azure PostgreSQL

- Retention Period:
  - 7-35 days (default is 7)
  - No native long term retention support

Azure PostgreSQL

- Availability:
  - Backup is stored in a geo-redundant storage
    - In General Purpose and Memory Optimized tiers
  - SLA: 99.99%

Azure Storage

- Object store
- Massively scalable
- Accessible via HTTP or HTTPS
- Client libraries for almost every language
- Durable and highly available

Azure Storage Types

Blobs	→	Object Store	This one we like ☺
Files	→	File shares for cloud and on-prem deployments	Related more to compute, quite low level
Queues	→	Queues (duh…)	We'll discuss this in the Messaging section
Tables	→	NoSQL data store	Similar to CosmosDB, but less optimized for performance and availability (cheaper, though…)
Disks	→	Storage volumes for Azure VMs	Managed by the VM, nothing to deal with here

Azure Blobs Storage

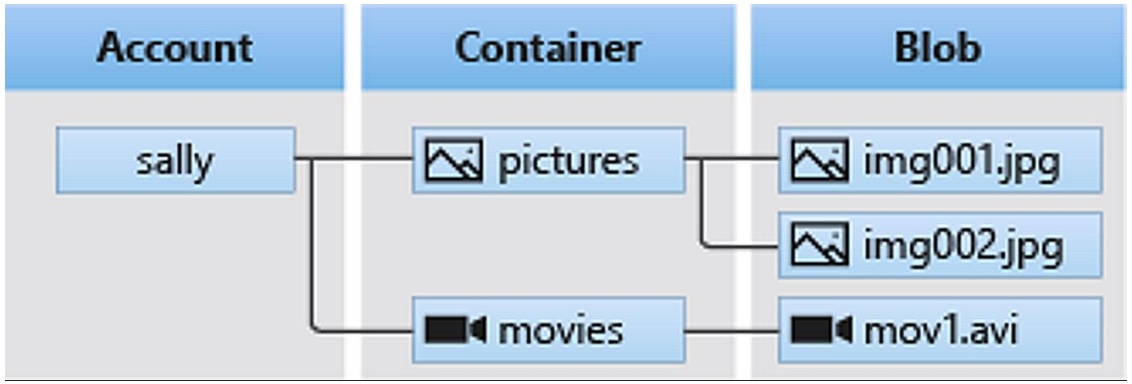
- Object store (Blob = Binary Large Object)
- Great for files, videos, documents, large texts etc.
- Up to 4.77TB per file (!), 190TB in preview (!!)
- Extremely cost effective
- Massively scalable
- Great availability options
- Extremely easy to use
- Usually used in conjunction with SQL / NoSQL database

Azure Blobs Storage

- Security:
  - IP firewall rules
  - Service Endpoints
  - Private Endpoints
  - Shared Access Signatures
  - Access Keys & Azure AD Authentication
  - Secure communication (TLS)
  - Data encrypted by default

Azure Blobs Storage

- Structure:



Azure Blobs Storage Redundancy

- 6 options:

LRS

Locally Redundant Storage

Data is synchronously copied 3 times within the same zone

ZRS

Zone Redundant Storage

Data is synchronously copied to 3 zones in the Region

GRS

Geo Redundant Storage

Data is synchronously copied 3 times within the same zone, and then copied asynchronously to paired Region.
Data in the secondary Region is accessible only after Failover process

GZRS

Geo-Zone Redundant Storage

Data is synchronously copied to 3 zones in the Region, and then copied asynchronously to paired Region.
Data in the secondary Region is accessible only after Failover process

RA-GRS

Read Access-Geo Redundant Storage

Data is synchronously copied 3 times within the same zone, and then copied asynchronously to paired Region.
There's a read-access to the data in the secondary Region

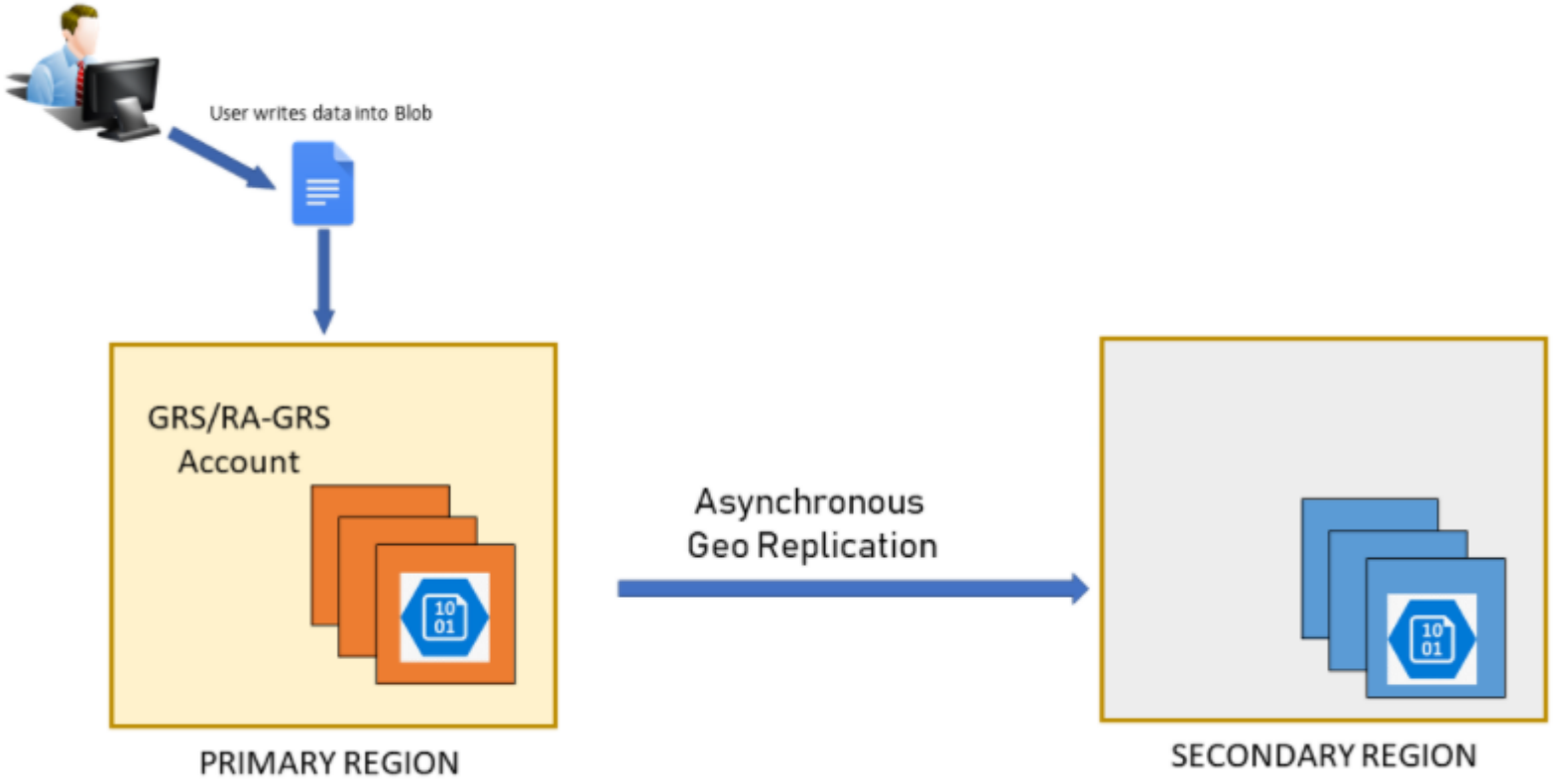
RA-GZRS

Read Access-Geo-Zone Redundant Storage

Data is synchronously copied to 3 zones within the same Region, and then copied asynchronously to paired Region.
There's a read-access to the data in the secondary Region

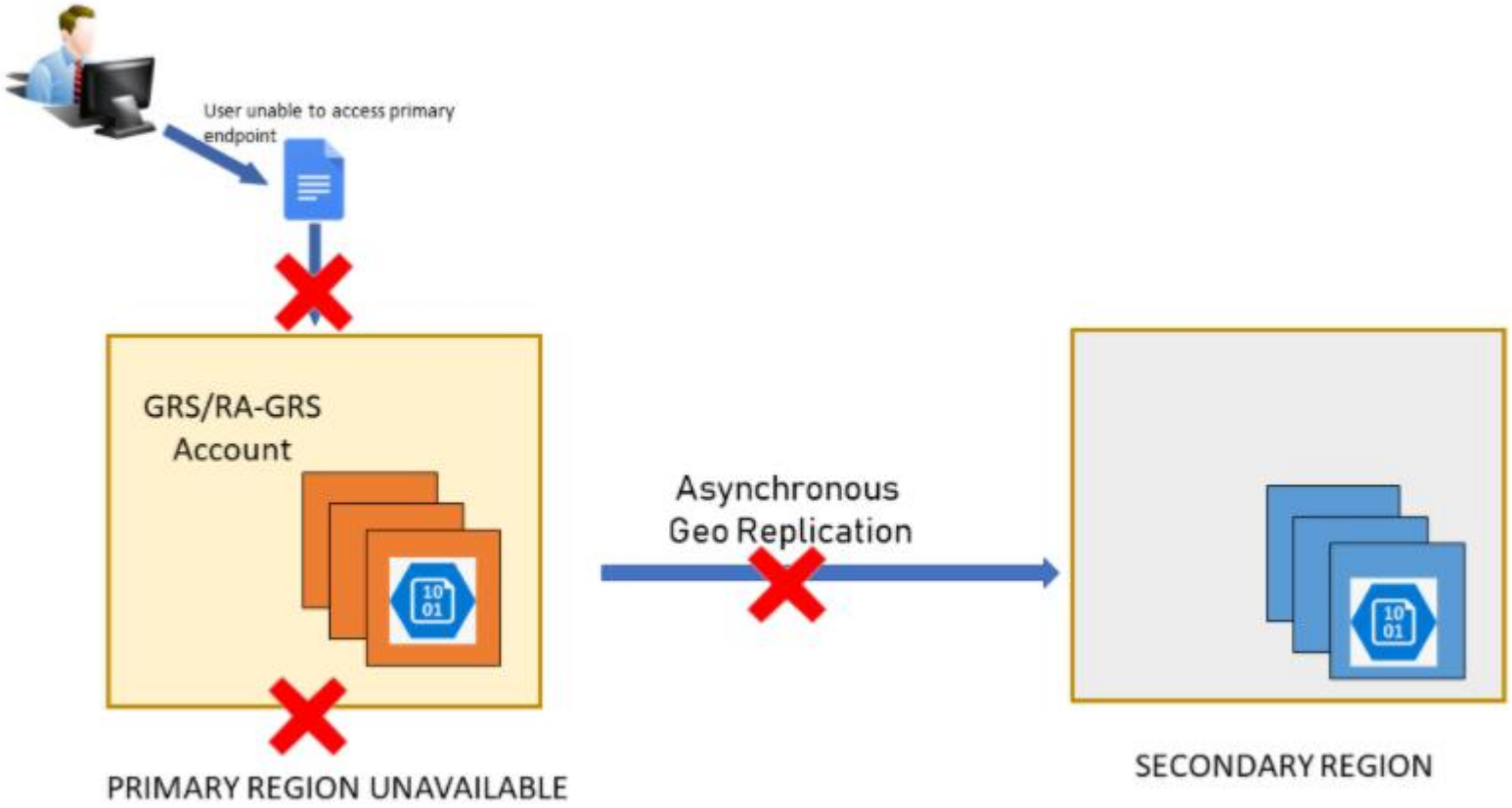
Azure Blobs Storage Failover

- Normal circumstances:



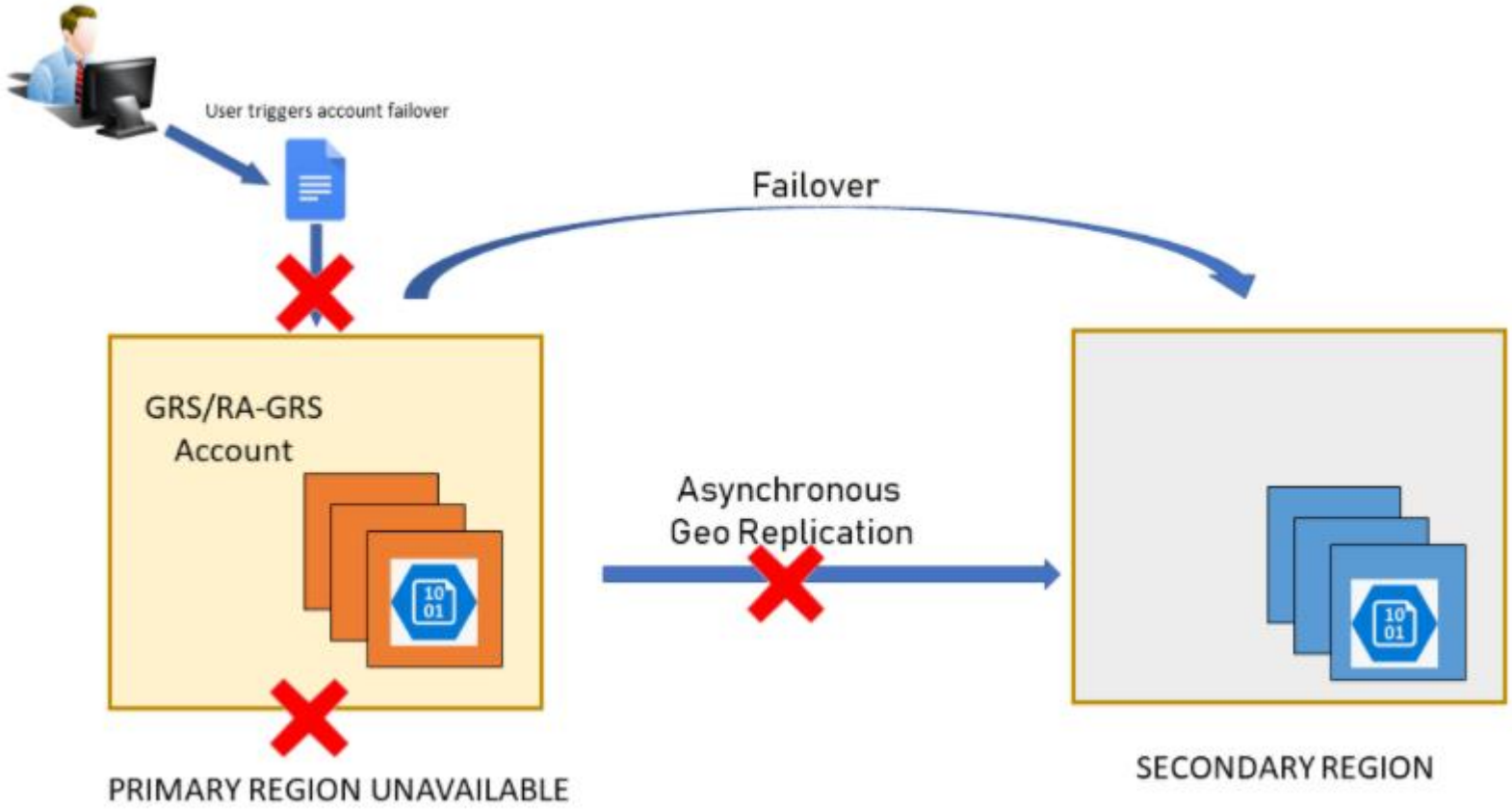
Azure Blobs Storage Failover

- Primary Region fails:



Azure Blobs Storage Failover

- Failover to the secondary Region:



Azure Blobs Storage Failover

- Can be initiated via the:
  - Portal
  - Azure CLI
  - PowerShell

Azure Blobs Storage Tiers

- Blobs are uploaded to one of three tiers:

Hot

- Data that's accessed frequently
- Best SLA (99.9%)
- Highest storage costs
- Lowest access costs
- Examples:
  - Photos to display
  - Documents to show

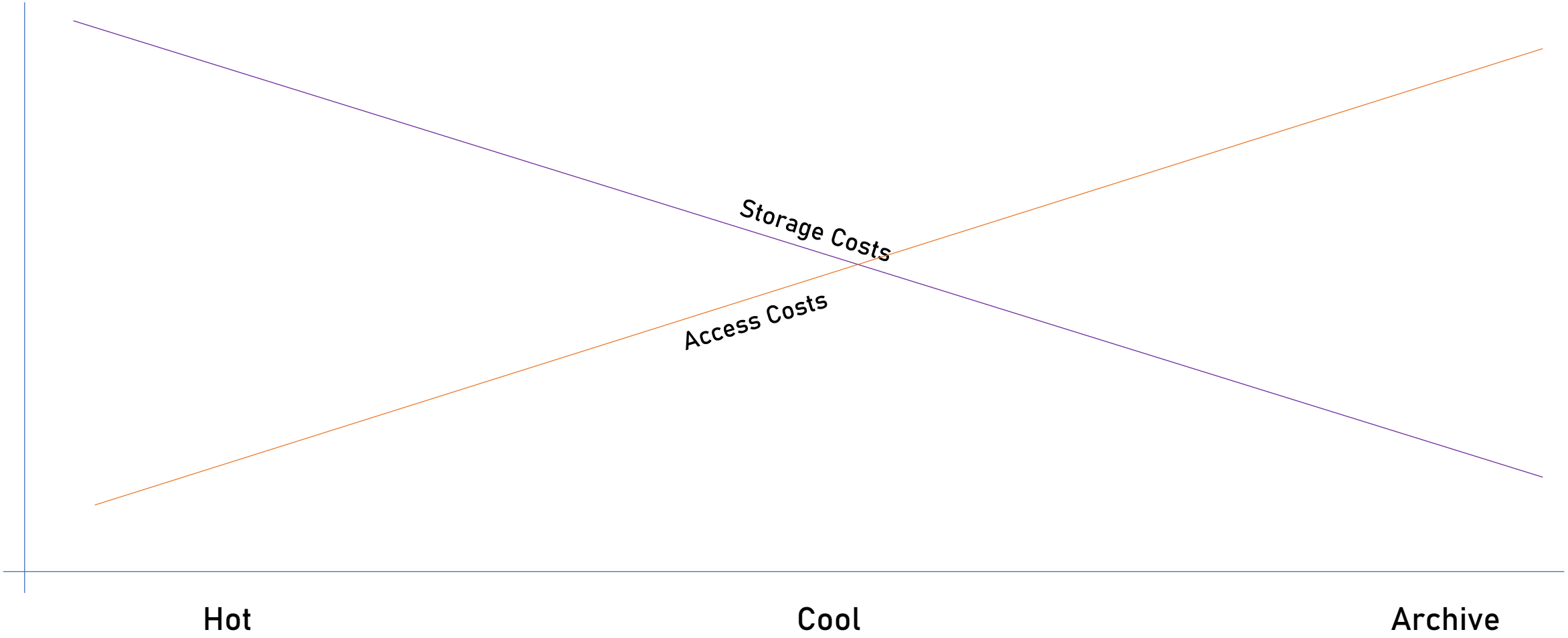
Cool

- Data that's accessed infrequently
- Slightly lower SLA (99%)
- Lower storage costs
- Higher access costs
- Must be stored for at least 30 days (or early deletion fees applied)
- Examples:
  - Short term backup
  - Data for future processing

Archive

- Data for archival
- Stored offline, no SLA
- Can take hours to retrieve
- Lowest storage costs
- Highest access costs
- Must be stored for at least 180 days (or early deletion fees applied)

Azure Blobs Storage Tiers



Azure Blobs Storage Tiers

- Retrieval time is the same in Hot and Cool tiers
- Archive tier does not support ZRS, GRS and RA-GRS redundancy
- Using RA-G(Z)RS, SLA improves to 99.99% (Hot) and 99.9% (Cool)
- Tier is set at account level, can be modified per blob
- Moving between tiers can be automated by lifecycle rules

Azure Blobs Storage Pricing

- Based on:
  - Redundancy option
  - Access tier
  - Capacity

Storage Accounts

REGION: West Europe

TYPE: Block Blob Storage

PERFORMANCE TIER: Standard

STORAGE ACCOUNT TYPE: General Purpose V2

REDUNDANCY: LRS

ACCESS TIER: Hot

Capacity

1000 GB

Savings Options

Save up to 38% on pay-as-you-go prices with 1-year or 3-year Azure Storage Reserved Capacity. Learn more about Azure Storage Reserved Capacity pricing.

- (●) Pay as you go
- ( ) 1 year reserved
- ( ) 3 year reserved

$19.60
Average per month
($0.00 charged upfront)

= $19.60
Average per month
($0.00 charged upfront)

Write Operations

100000 Operations × $0.054 Per 10,000 operations = $0.54

The following API calls are considered Write Operations: PutBlob, PutBlock, PutBlockList, AppendBlock, SnapshotBlob, CopyBlob and SetBlobTier (when it moves a Blob from Hot to Cool, Cool to Archive or Hot to Archive).

List and Create Container Operations

100000 Operations × $0.054 Per 10,000 operations = $0.54

Storage Accounts

REGION: West Europe

TYPE: Block Blob Storage

PERFORMANCE TIER: Standard

STORAGE ACCOUNT TYPE: General Purpose V2

REDUNDANCY: LRS

ACCESS TIER: Cool

Capacity

1000 GB

Early deletion fees may apply and are not included. Learn more about early deletion fees.

Savings Options

Save up to 38% on pay-as-you-go prices with 1-year or 3-year Azure Storage Reserved Capacity. Learn more about Azure Storage Reserved Capacity pricing.

- Pay as you go
- 1 year reserved
- 3 year reserved

$10.00
Average per month
($0.00 charged upfront)

= $10.00
Average per month
($0.00 charged upfront)

Write Operations

100000 Operations × $0.100 Per 10,000 operations = $1.00

The following API calls are considered Write Operations: PutBlob, PutBlock, PutBlockList, AppendBlock, SnapshotBlob, CopyBlob and SetBlobTier (when it moves a Blob from Hot to Cool, Cool to Archive or Hot to Archive).

List and Create Container Operations

100000 Operations × $0.054 Per 10,000 operations = $0.54

Storage Accounts

REGION: West Europe

TYPE: Block Blob Storage

PERFORMANCE TIER: Standard

STORAGE ACCOUNT TYPE: General Purpose V2

REDUNDANCY: RA-GRS

ACCESS TIER: Cool

Capacity

1000 GB

Early deletion fees may apply and are not included. Learn more about early deletion fees.

Savings Options

Save up to 38% on pay-as-you-go prices with 1-year or 3-year Azure Storage Reserved Capacity. Learn more about Azure Storage Reserved Capacity pricing.

- (●) Pay as you go
- ( ) 1 year reserved
- ( ) 3 year reserved

$25.00
Average per month
($0.00 charged upfront)

= $25.00
Average per month
($0.00 charged upfront)

Write Operations

100000 Operations × $0.200 Per 10,000 operations = $2.00

The following API calls are considered Write Operations: PutBlob, PutBlock, PutBlockList, AppendBlock, SnapshotBlob, CopyBlob and SetBlobTier (when it moves a Blob from Hot to Cool, Cool to Archive or Hot to Archive).

List and Create Container Operations

100000 Operations × $0.108 Per 10,000 operations = $1.08

Azure Redis

- Managed Redis on Azure
- Provides lightning-fast in-memory, distributed cache
- Great for short-lived, frequently accessed data
  - ie. shopping cart, stock quotes
- Fully compatible with OSS Redis (community edition) and Enterprise Redis – depends on service tiers

Azure Redis

- Security:
  - IP firewall rules
  - Service Endpoints
  - Private Endpoints
  - Secure communication (TLS)

Azure Redis Service Tiers

Basic	Based on a single VM, no SLA, no distribution. Good for dev/test
Standard	Based on two VMs, replicated. SLA – Up to 99.9%
Premium	High-performance, better throughput, lower latency. SLA – Up to 99.95%
Enterprise	Based on Redis Enterprise, offers additional features (RediSearch, RedisBloom and more). SLA – Up to 99.99%
Enterprise Flash	Uses non-volatile memory. Reduces storage cost. SLA – Up to 99.99%

Azure Redis Pricing

- Based on:
  - Tier
  - Memory

Azure Cache for Redis

REGION: West US

TIER: Basic

INSTANCE: C0: 250 MB cache, $0.022/hour

1 Instances × 730 Hours

Upfront cost	$0.00
Monthly cost	$16.06

Azure Cache for Redis

REGION:
West US

TIER:
Premium

INSTANCE:
P3: 26624 MB cache, $2.218/hour

Savings Options

- (●) Pay as you go
- ( ) 1 year reserved (~36% savings)
- ( ) 3 year reserved (~55% savings)

$1,619.14
Average per month
($0.00 charged upfront)

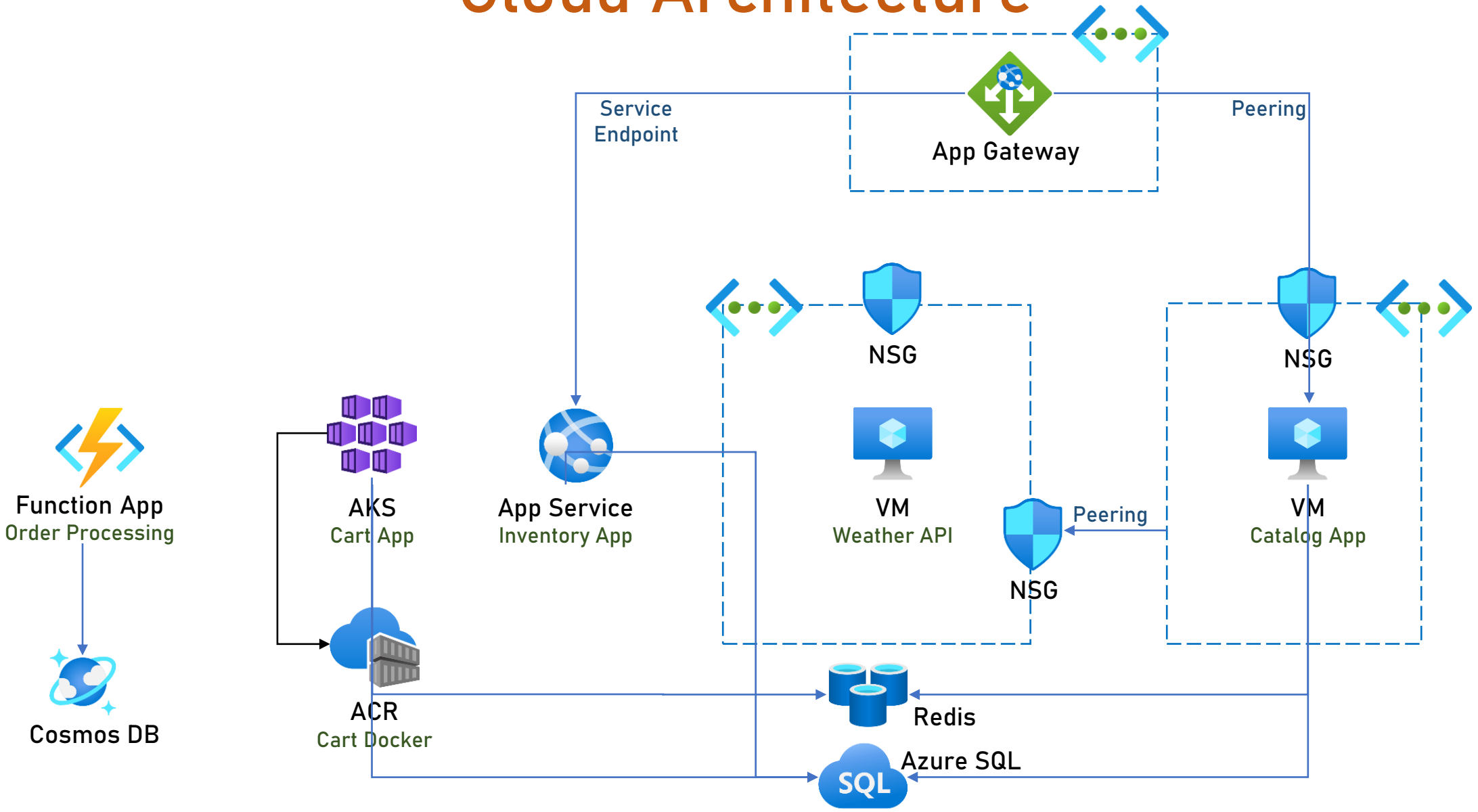
= $1,619.14
Average per month
($0.00 charged upfront)

1 × 730 Hours
Instances

Upfront cost	$0.00
Monthly cost	$1,619.14

ReadIt!

Cloud Architecture



Are we done?

- Nope ☺
  - The Orders Function is publicly available and synchronous
  - The inventory page is open for everyone
  - We don't really know how the app is functioning
  - The website is not redundant – what happens if the whole region goes down?

Selecting Data Store Solution

Data Type	Used For…	Examples	Options in Azure
Relational	Structured data	Items in store, demographic data	Azure SQL, MySQL, PostgreSQL
NoSQL	Semi-structured data	Reviews, Log records, when flexibility is required	Cosmos DB (with SQL, Mongo, Azure Table API)
Graph	Data representing relationships	Family tree	Cosmos DB (with Gremlin API)
Blob	Files, videos, docs	Items' photos	Azure Blob Storage

Messaging in Azure

Memi Lavi
www.memilavi.com

Messaging in Azure

- Messaging is extremely important aspect of Software Architecture
- Must be able to handle load, throughput, and have great latency
- A core part of every Microservices architecture

Messaging in Azure

- Azure has 4 fully managed messaging services

Storage Queue

Service Bus

Events Grid

Event Hubs

Storage Queue

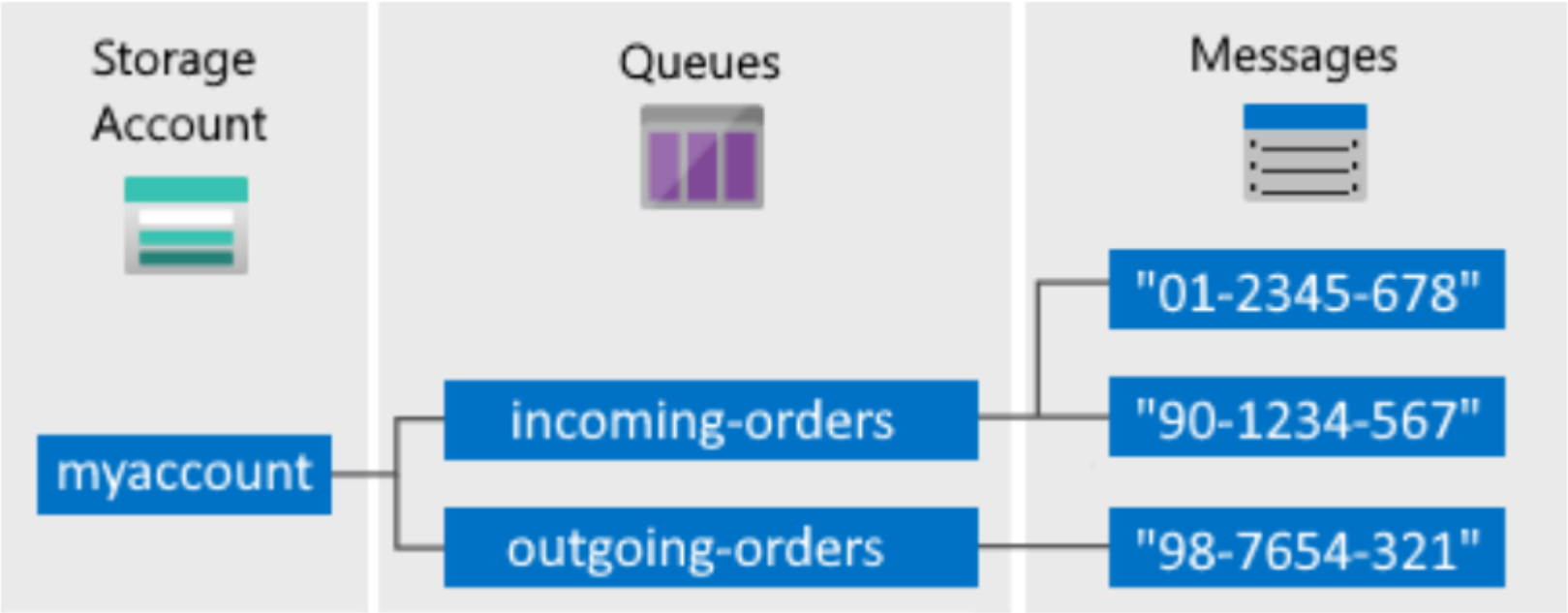
- Part of Azure Storage Account
- The simplest queue implementation
- Create queue -> Send Message -> Receive message
- No special pricing for queue, included in Storage Account
- Same for availability

Storage Queue

- Performance:
  - Requests (1KB msg)
    - 20K msgs / sec / account
    - 2K msgs / sec / queue
- Max msg size: 64KB

Storage Queue

- Architecture:



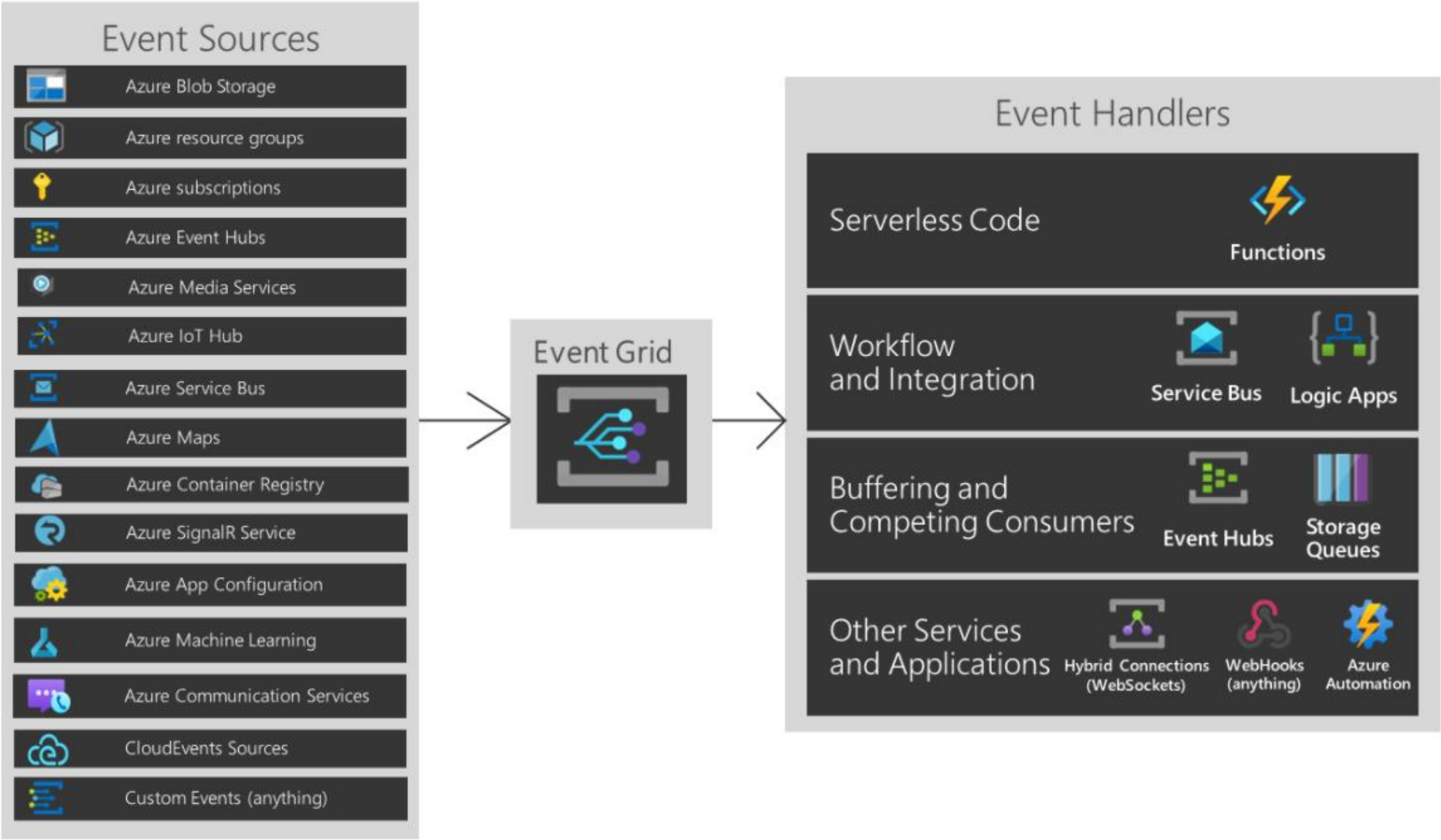
Storage Queue

- Development:
  - Client libraries for many development languages
    - .NET, Java, Python, NodeJS, C++, PHP, Ruby
  - Extremely simple object model

Event Grid

- Allows building event-based architectures
- Publishes events to interested parties
- No queue / no order
- Strong integration with many Azure services
- Cost effective, simple pricing
- No tiers, HA is built in

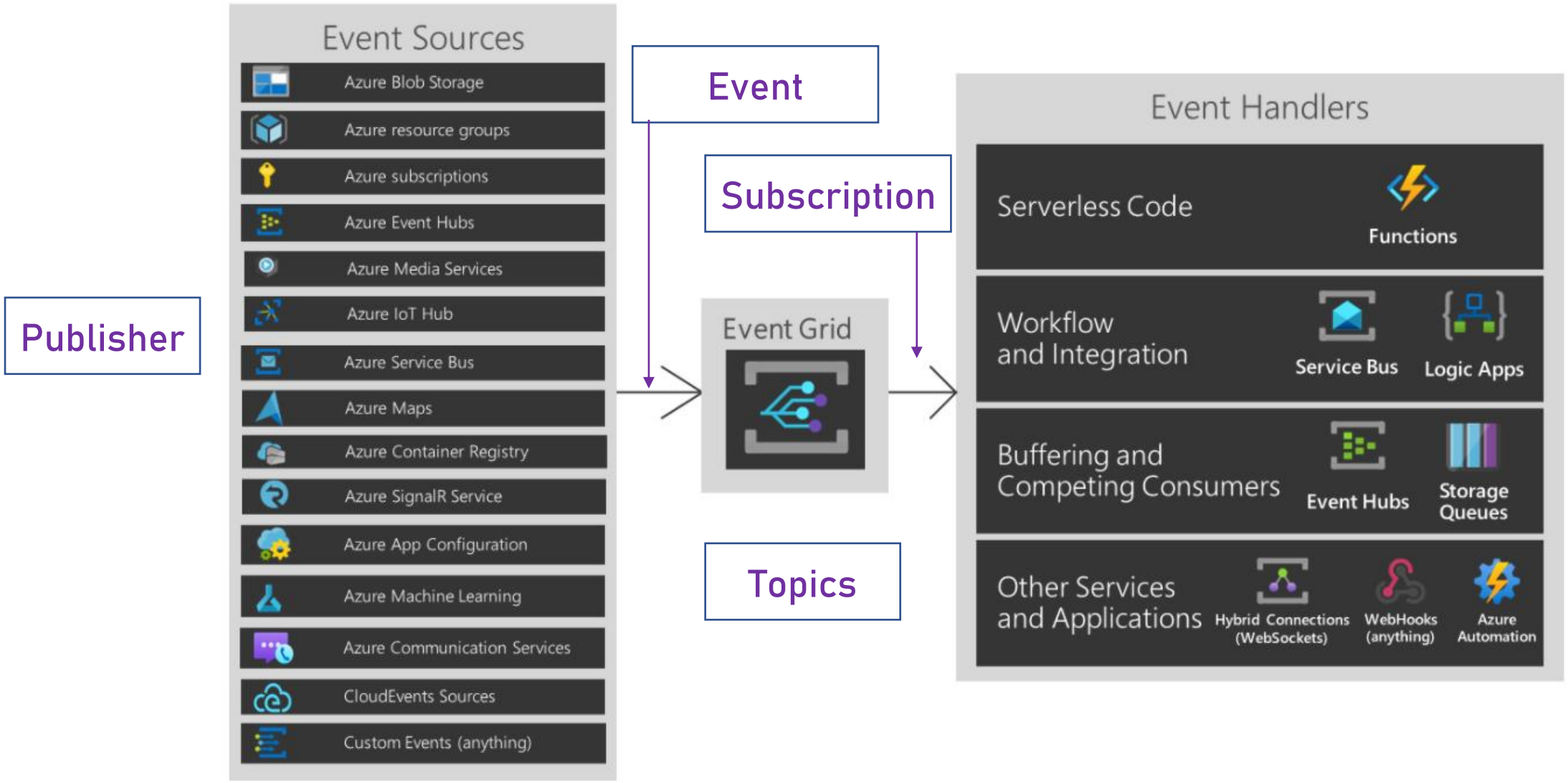
Event Grid


Event Sources
Azure Blob Storage
Azure resource groups
Azure subscriptions
Azure Event Hubs
Azure Media Services
Azure IoT Hub
Azure Service Bus
Azure Maps
Azure Container Registry
Azure SignalR Service
Azure App Configuration
Azure Machine Learning
Azure Communication Services
CloudEvents Sources
Custom Events (anything)
Event Grid
Event Handlers
Serverless Code
Functions
Workflow and Integration
Service Bus
Logic Apps
Buffering and Competing Consumers
Event Hubs
Storage Queues
Other Services and Applications
Hybrid Connections (WebSockets)
WebHooks (anything)
Azure Automation

Terminology

Event	What happened. Examples: Storage blob added, IOT telemetry received
Publisher	Who created the event. Examples: Microsoft, my organization
Event Source	Where the event happened. Examples: Storage account, IOT Hub
Topic	Where the event is sent. Used to group related events.
Subscription	Which events interest me. Examples: Storage blob added, IOT telemetry received
Event Handler	Where the event is sent. Examples: Azure Function, Event Hubs etc.

Event Grid


Publisher
Event Sources
Azure Blob Storage
Azure resource groups
Azure subscriptions
Azure Event Hubs
Azure Media Services
Azure IoT Hub
Azure Service Bus
Azure Maps
Azure Container Registry
Azure SignalR Service
Azure App Configuration
Azure Machine Learning
Azure Communication Services
CloudEvents Sources
Custom Events (anything)
Event
Subscription
Topics
Event Grid
Event Handlers
Serverless Code
Functions
Workflow and Integration
Service Bus
Logic Apps
Buffering and Competing Consumers
Event Hubs
Storage Queues
Other Services and Applications
Hybrid Connections (WebSockets)
WebHooks (anything)
Azure Automation

Event Grid

- SLA:
  - 99.99%
- Max event size:
  - 1MB

Event Grid

- Performance:
  - 10,000,000 events / sec
  - 5,000 events / sec / topic
- Latency:
  - Subsecond end-to-end latency in the 99th percentile

Event Grid Pricing

- Based on:
  - Number of operations
    - First 100K operations are free

Event Grid

REGION:

West US 2

First 100,000 operations are free

1000000

Operations per month

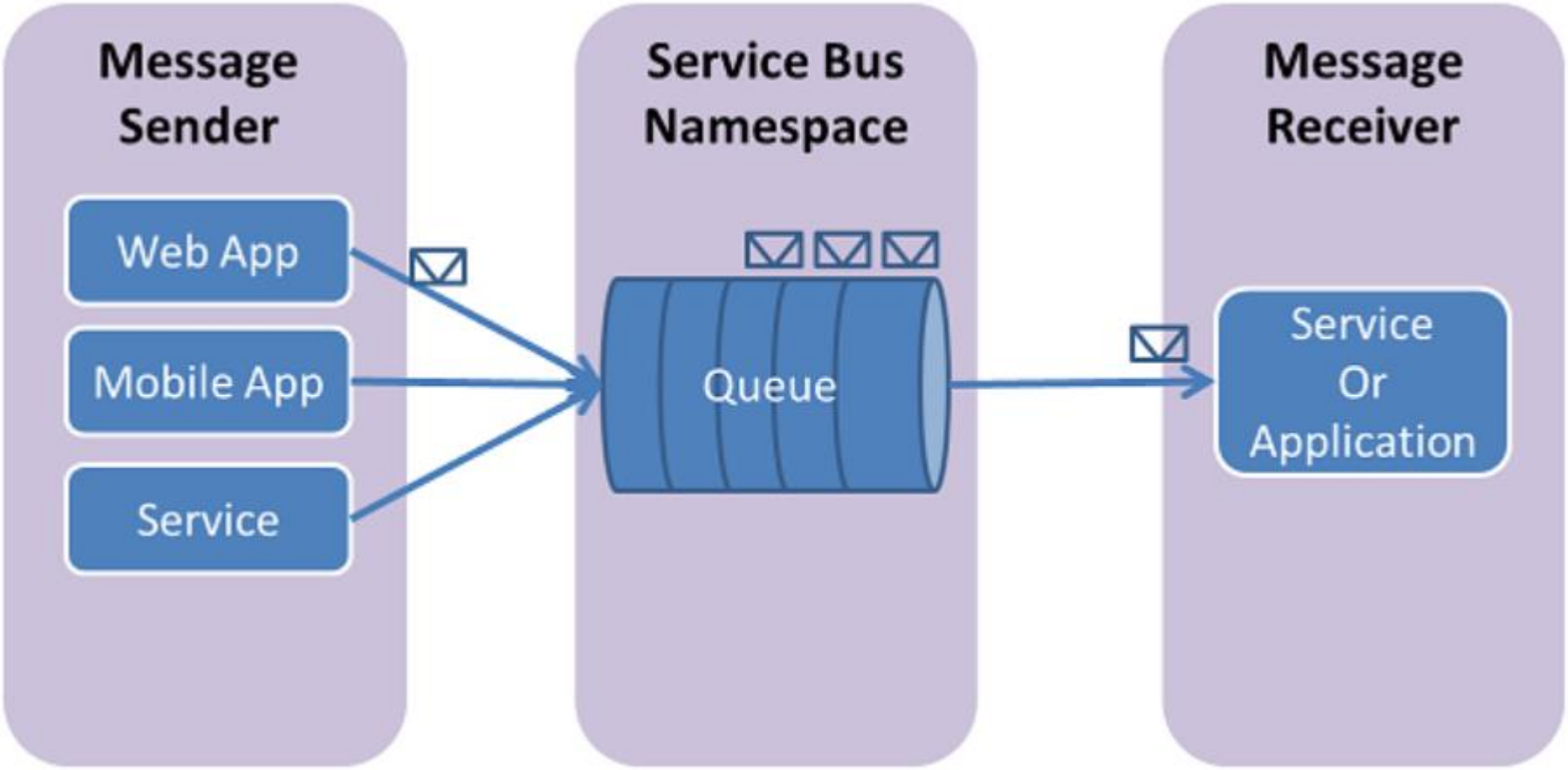
= $0.54

Upfront cost	$0.00
Monthly cost	$0.54

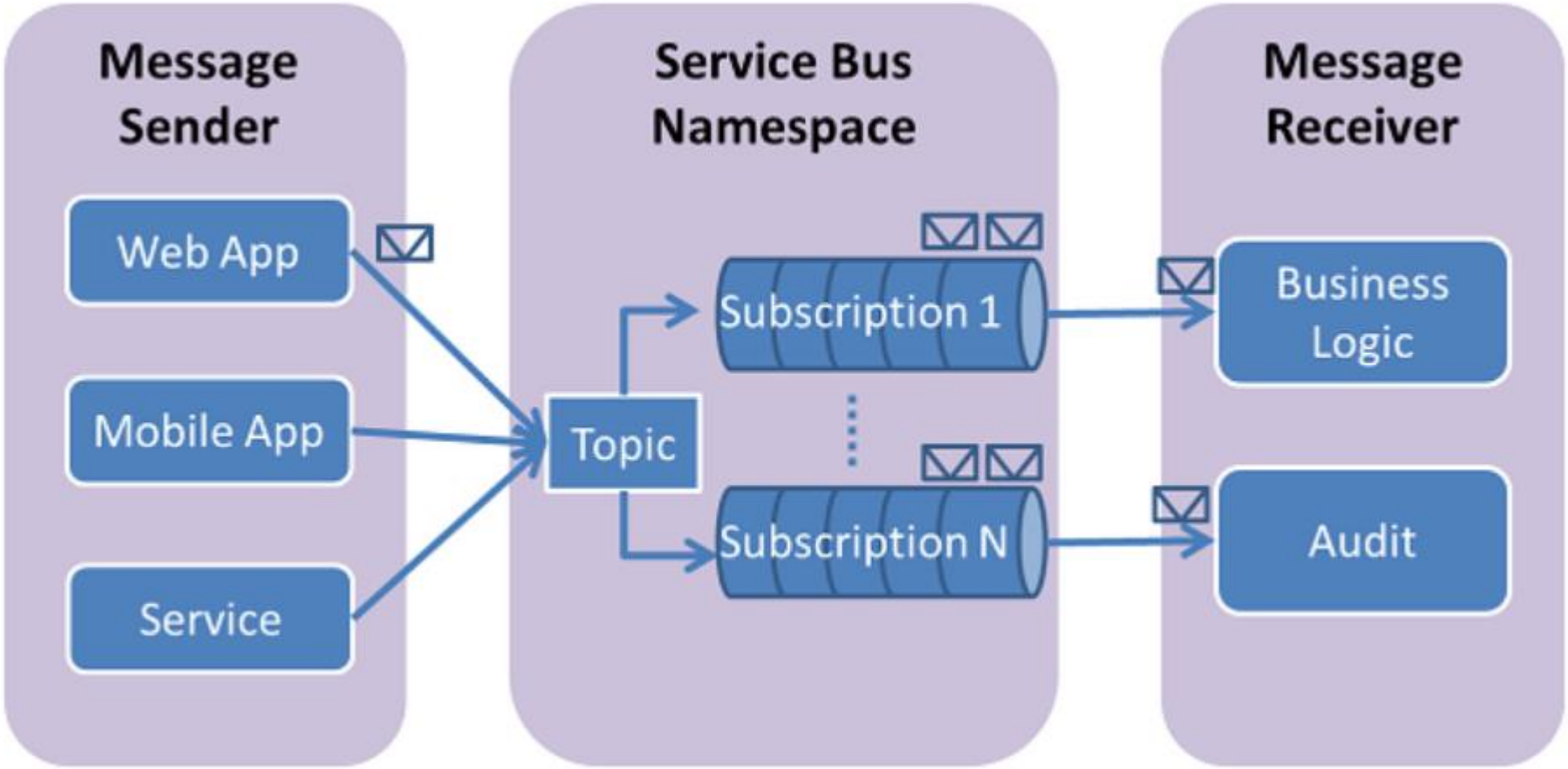
Service Bus

- Fully managed, full blown message queueing service
- Durable
- Supports point-to-point (Queue) and pub/sub (Topic) scenarios
- Compatible with AMQP protocol
- Compatible with JMS 2.0 API (Premium only)

Service Bus Queues



Service Bus Topics



Service Bus

- Advanced features:
  - Message sessions (guarantees FIFO)
  - Dead-letter queue
  - Scheduled delivery
  - Transactions
  - Duplicate detection
  - And more…

Service Bus

- Availability:
  - SLA: 99.9%
  - Can be configured for geo-disaster recovery

Service Bus

- Security:
  - IP Firewall rules
  - Service endpoints
  - Private endpoints

Service Bus Tiers

- Basic, Standard, Premium

FEATURE	BASIC	STANDARD	PREMIUM
Queues	✓	✓	✓
Scheduled messages	✓	✓	✓
Topics		✓	✓
Transactions		✓	✓
De-duplication		✓	✓
Sessions		✓	✓
ForwardTo/SendVia		✓	✓
Message Size	256 KB	256 KB	1 MB
Resource isolation			✓
Geo-Disaster Recovery (Geo-DR)			✓ *Requires additional Service Bus Premium namespaces in another region.
Availability Zones (AZ) support			✓

Service Bus Pricing

- Based on:
  - Tier
  - No. of operations

Service Bus

REGION:

West Europe

TIER:

Standard

Messaging operations

10 Million/month + $0.013 Base charge × 730 Hours = $9.81

Service Bus

REGION:

West Europe

TIER:

Premium

Service Bus Premium runs in dedicated resources to provide higher throughput and more consistent performance.

Daily message units:

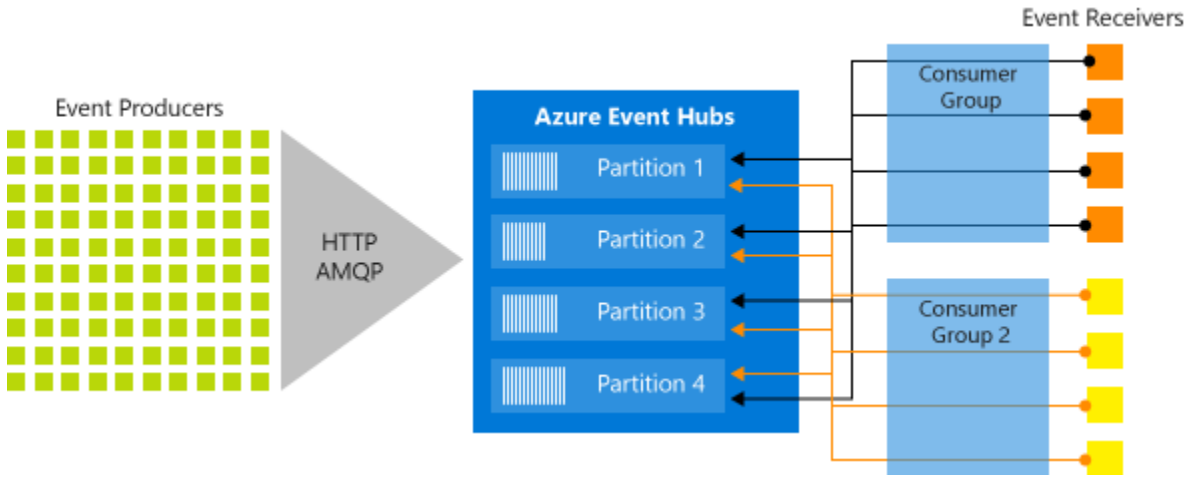
2 × $0.93 Per message unit × 730 Hours = $1,354.15

Upfront cost	$0.00
Monthly cost	$1,354.15

Event Hubs

- Big Data streaming platform and event ingestion service
- Note: No “messaging” in the description
- Basically a managed Kafka implementation
- Can receive millions of events per second

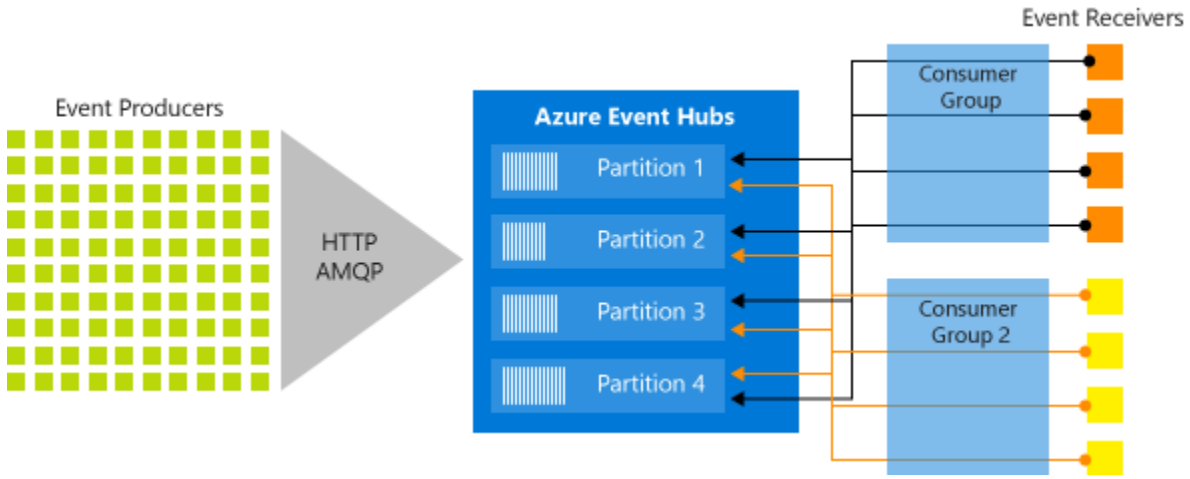
Event Hubs Architecture



Event Producers

- Components generating the events
- Can be done by anyone with the client / HTTP client
- Simple connection and API

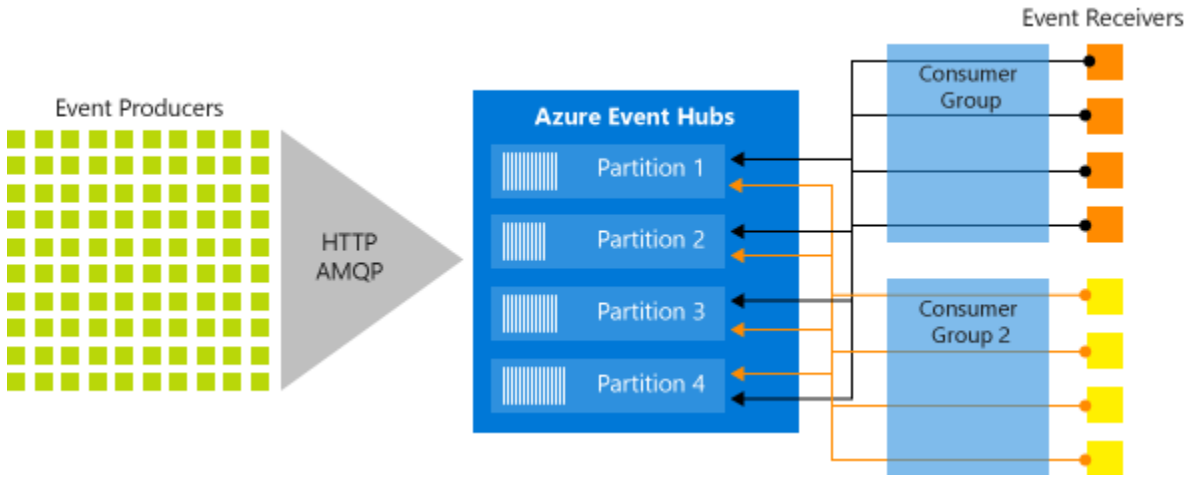
Event Hubs Architecture



Partition

- Single event stream
- Can think of it as a single queue
- Guarantees order
- Limited availability
- Better to spread messages across partitions to improve availability
- …but then order is not guaranteed
- Max 32 partitions on a single Event Hubs

Event Hubs Architecture



Consumer Group

- Logical group of receivers, belong to the same application
- Example:
  - Receivers for processing telemetry = Consumer Group
  - Receivers for storing the telemetry = Consumer Group
- Event receiving is done via AMQP protocol

Event Hubs

- SLA:
  - Basic and Standard tier: 99.95%
  - Dedicated: 99.99%

Event Hubs Throughput Units

- Throughput is measured in Throughput Units (TU)
- 1 TU =
  - Ingress (Input) – 1MB / sec or 1000 events / sec
  - Egress (Output) – 2MB / sec or 4096 events / sec
- Prepurchased, billed by the hour

Event Hubs Pricing

- Based on:
  - Tier
  - Ingress
  - TU

Event Hubs

REGION: East US

TIER: Basic

Maximum throughput units: 20. Up to 1 MB per second of ingress events. Up to 2 MB per second of egress events.

Ingress

10 Million events × $0.028 Per million = $0.28

Throughput

1 Throughput units × 730 Hours × $0.015 Per unit/hour = $10.95

Upfront cost	$0.00
Monthly cost	$11.23

Event Hubs

REGION: East US

TIER: Dedicated

Minimum hours charged are 4. Ingress and throughput charges are included.

730	Hours	×	4 Capacity Units	×	$6.849 Per hour	=	$19,999.080

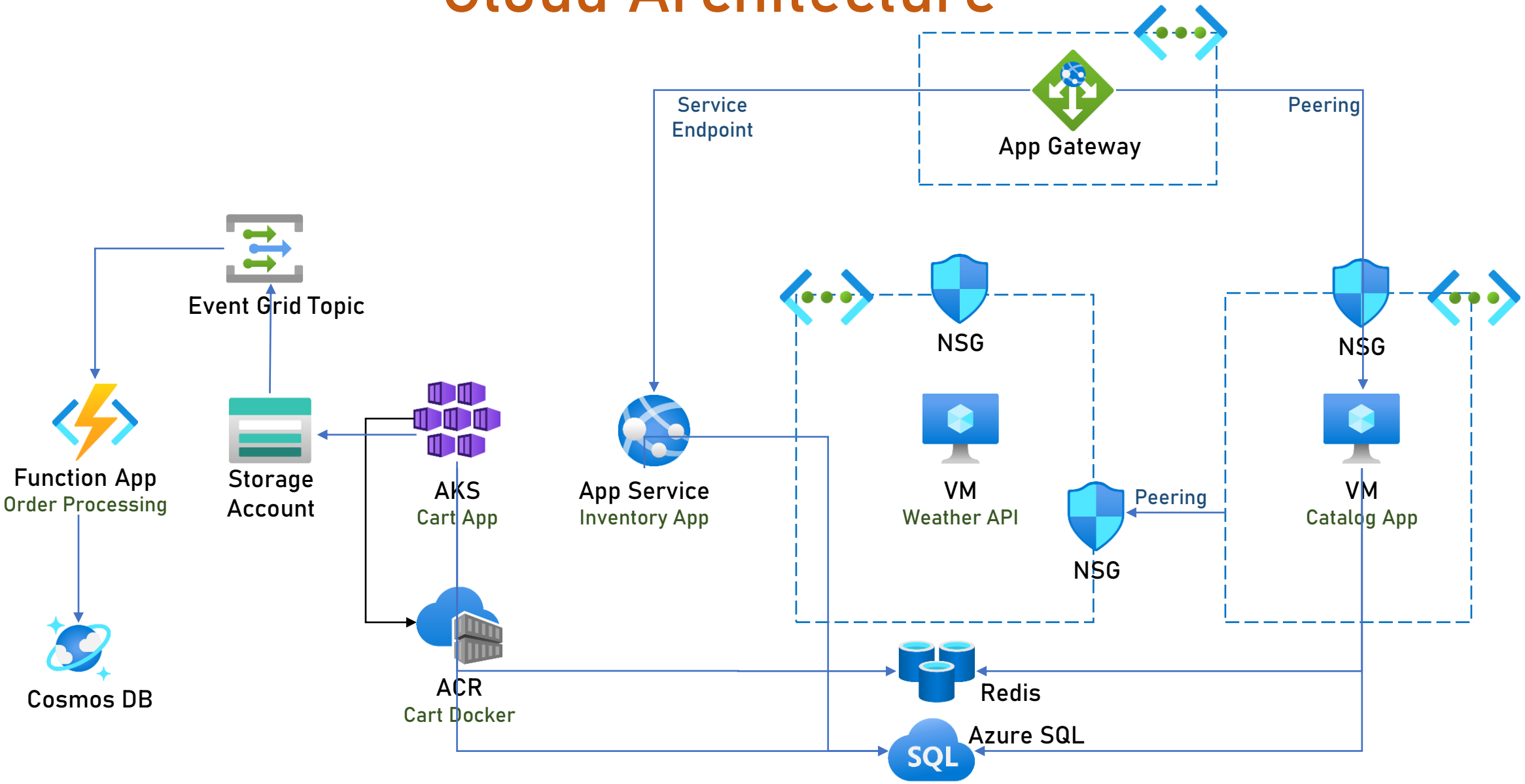
Upfront cost	$0.00
Monthly cost	$19,999.08

Selecting Messaging Solution

Service	Used For…	Guarantees Order	Max Msg Size	And also…
Storage Queue	Dead simple queueing	Yes	64KB	Extremely simple, no additional cost
Event Grid	Event driven architectures	No	1MB	Great integration with other services
Service Bus	Advanced queueing solutions	Yes	256KB	Advanced messaging features, durable
Event Hubs	Big data streaming	Yes	1MB	Low latency, designed for heavy load

ReadIt!

Cloud Architecture



Azure AD

Memi Lavi
www.memilavi.com

Azure AD

- Short for Azure Active Directory
- Central identity and access management cloud service
- Used to manage access to thousands of apps
  - Among them – the Azure Portal
- Secure, robust, intelligent

Azure AD

- Advanced features:
  - MFA
  - Conditional Access
  - Device management
  - Hybrid identity
  - Identity protection
  - Monitoring and reports
  - And lots more…

Azure AD

- We're interested mainly in:
  - Control access to Azure resources
    - By setting up users, groups, roles
    - Not entirely architecture- and dev- related, but still important
  - Use Azure AD to add authentication to our apps
  - Can be done also via Azure AD B2C

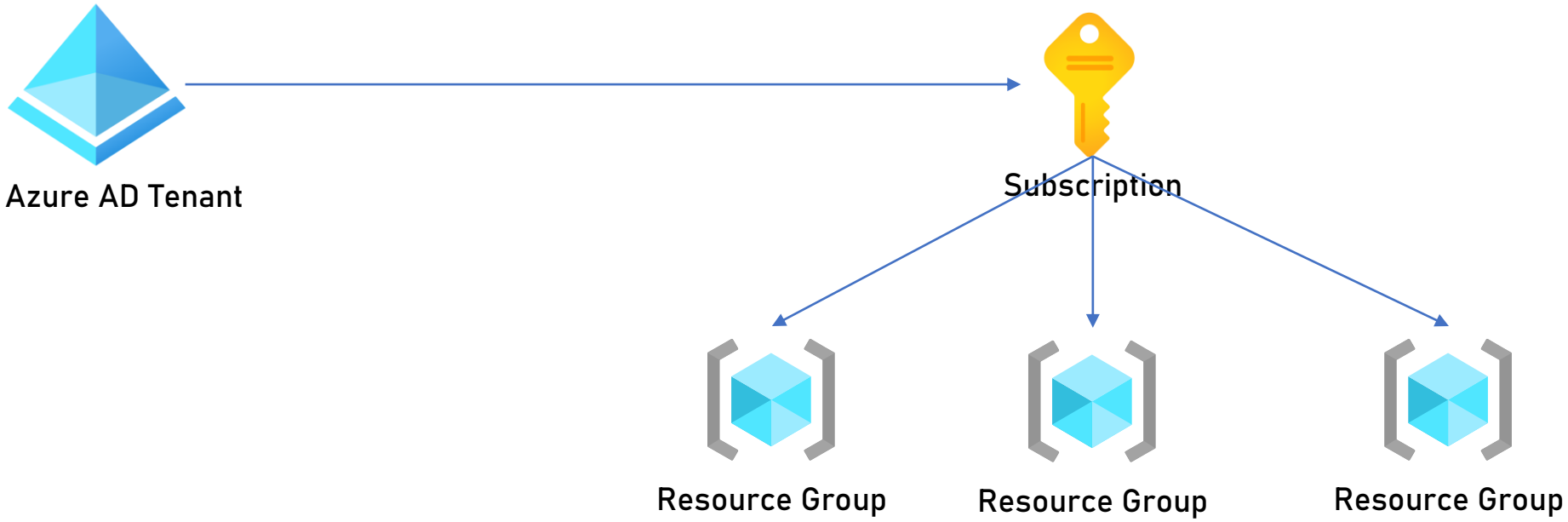
Azure AD Figures

- Integrates with more than 2,800 apps
- Manages more than 1.2 billion identities
- Processes over 8 billion authentications every day
- Secured using 3,500 security experts in Microsoft
- …which invests more than $1bn annually on cybersecurity
- The largest identity and access management service in the world

Tenant

- A specific instance of Azure AD containing accounts and groups
- Called also Directory
- Is NOT part of the subscription hierarchy
  - Exists beside the subscription
  - For new subscriptions, a new tenant is created automatically
- A tenant can be assigned to multiple subscriptions

Tenant


Azure AD Tenant
Subscription
Resource Group
Resource Group
Resource Group

Users and Groups

- Two of the main three objects managed by Azure AD
  - The 3rd one is Roles (later…)
- Manages and stores the users that are part of the tenant
- Groups the users in Groups
  - Examples: IT Admins, Developers, etc.
  - Allows defining roles to groups instead of each user

Azure AD Licenses

- Azure AD Licenses have great effect on the functionality and price of Azure AD
- Important to understand the differences and recommend the right solution

Azure AD Licenses

	Free	Premium 1	Premium 2
Max Objects	500,000	Unlimited	Unlimited
Users & Groups	X	X	X
MFA	X (All or nothing)	X (With Conditional Access)	X (With Conditional Access)
Dynamic Groups		X	X
Conditional Access		X	X
Risk Detention			X
Risk based Conditional Access			X
Privileged Identity Management (PIM)			X
Price	Free	6$ user / month	9$ user / month

Azure AD Security Defaults

- Increases protection of the organization in the Free tier
- Adds preconfigured security settings:
  - Requiring all users to use MFA (block 99.9% of account compromises)
  - Blocks legacy authentication
  - And more…
- No additional cost (so…still free ☺)
- For more fine-grained management – use Conditional Access (P1)

RBAC in Azure

- In order to perform any operation, or access any data in Azure you have to have the appropriate role
- If you want to:
  - Create resource groups
  - Access data in SQL
  - See metrics of App Service
- … then you have to have the right role
- If you don't – you'll get an empty portal

RBAC in Azure

- In general, three types of roles:

Owner → Can perform any action on the resource, including assigning roles to it

Contributor → Can perform any action on the resource, but cannot assign roles to it

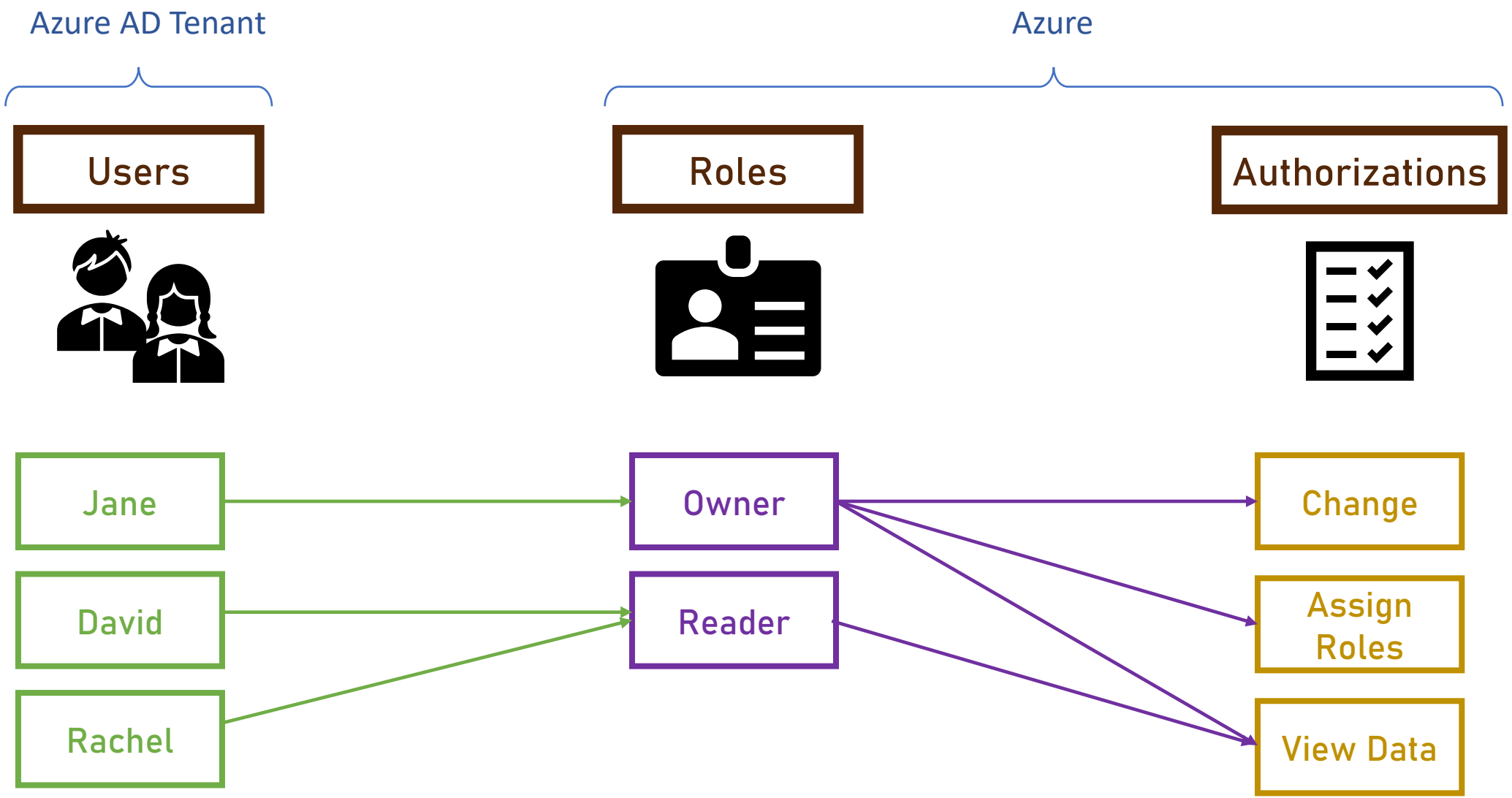
Reader → Can only view data, but cannot change anything

RBAC in Azure

- Examples:

Virtual Machine Contributor	Can manage virtual machines
Cosmos DB Account Reader	Can read Azure Cosmos DB account data
Service Bus Data Owner	Allows full access to Service Bus resources

RBAC in Azure



RBAC in Azure

- It's always better to assign roles to groups and not individual users
- Easier maintenance

Managed Identities

- The ability to assign Azure AD identity to Azure resource
- The resource can connect to other Azure resources using this identity
- No need to handle credentials (usernames, passwords etc.)

Managed Identities

- Two types of Managed Identities:
  - System assigned – Managed by Azure, tied to the resource's lifecycle (when the resource is deleted – so is the identity)
  - User assigned – Managed by the user. Can be assigned to multiple resources, not tied to any lifecycle

Managed Identities

- Resources that can be assigned Managed Identity:
  - App Service
  - Virtual Machine
  - Event Grid
  - Function
  - And more…

Managed Identities

- Resources that can be authorized using Managed Identity:
  - SQL
  - Event Hubs
  - Service Bus
  - Storage
  - Key Vault
  - And more…

Using Azure AD on Our App

- Azure AD can be used as authentication engine on other apps
- Not just the Azure Portal
- It can be used on our own app!

Using Azure AD on Our App

- The process:
  - Register the app in Azure AD
  - Add code to use Azure AD as authentication engine
    - For App Services – can be configured via the Portal

Using Azure AD on Our App

- The authentication:
  - Uses OAuth and JWT

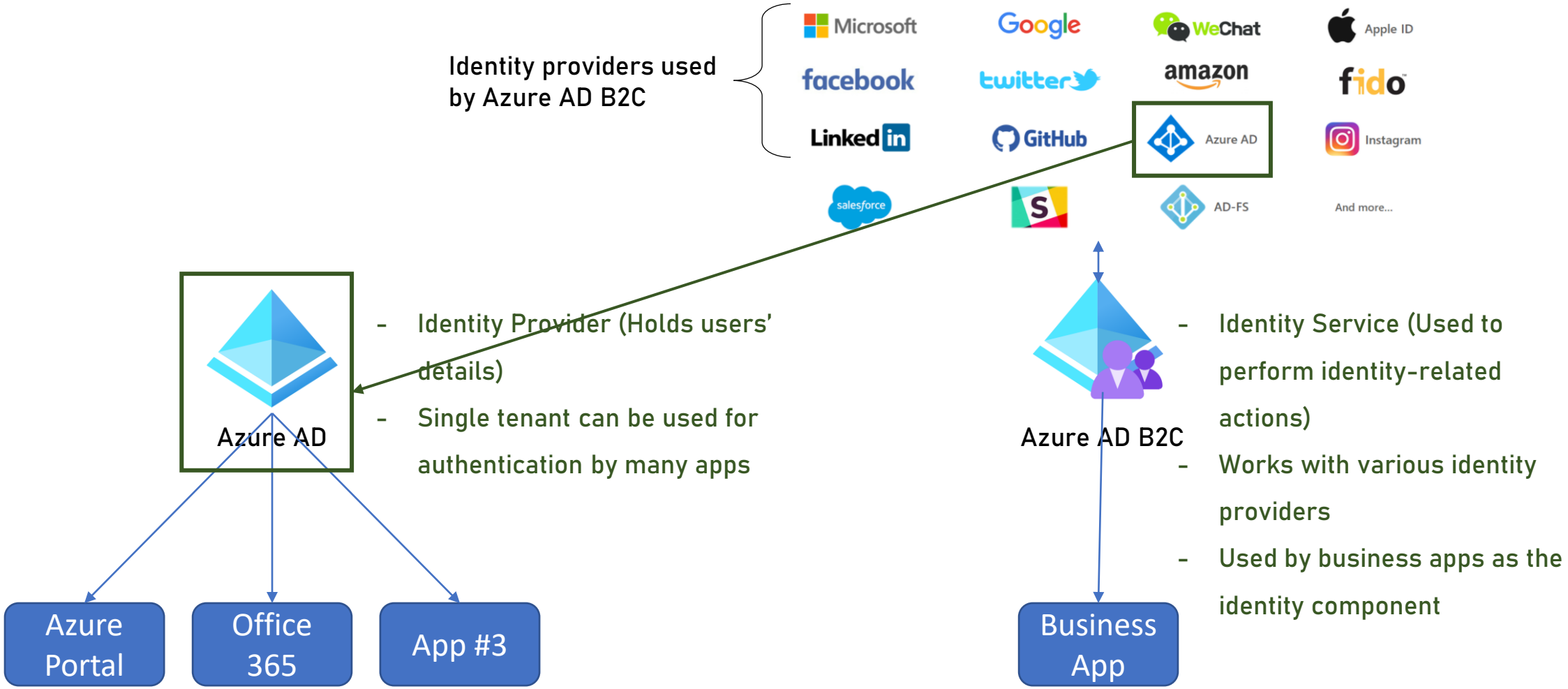
Azure AD B2C

- Identity-as-a-service for your application
- A Business-to-Customer (B2C) service
- Enables integrating identity services in your app
- Works with various identity providers
- Provides various user flows
- Enables customization

Azure AD B2C

- Identity services provided by Azure AD B2C:
  - Sign Up
  - Sign In
  - Log Out
  - Reset Password
  - And more…

Azure AD B2C vs Azure AD



Authentication Features

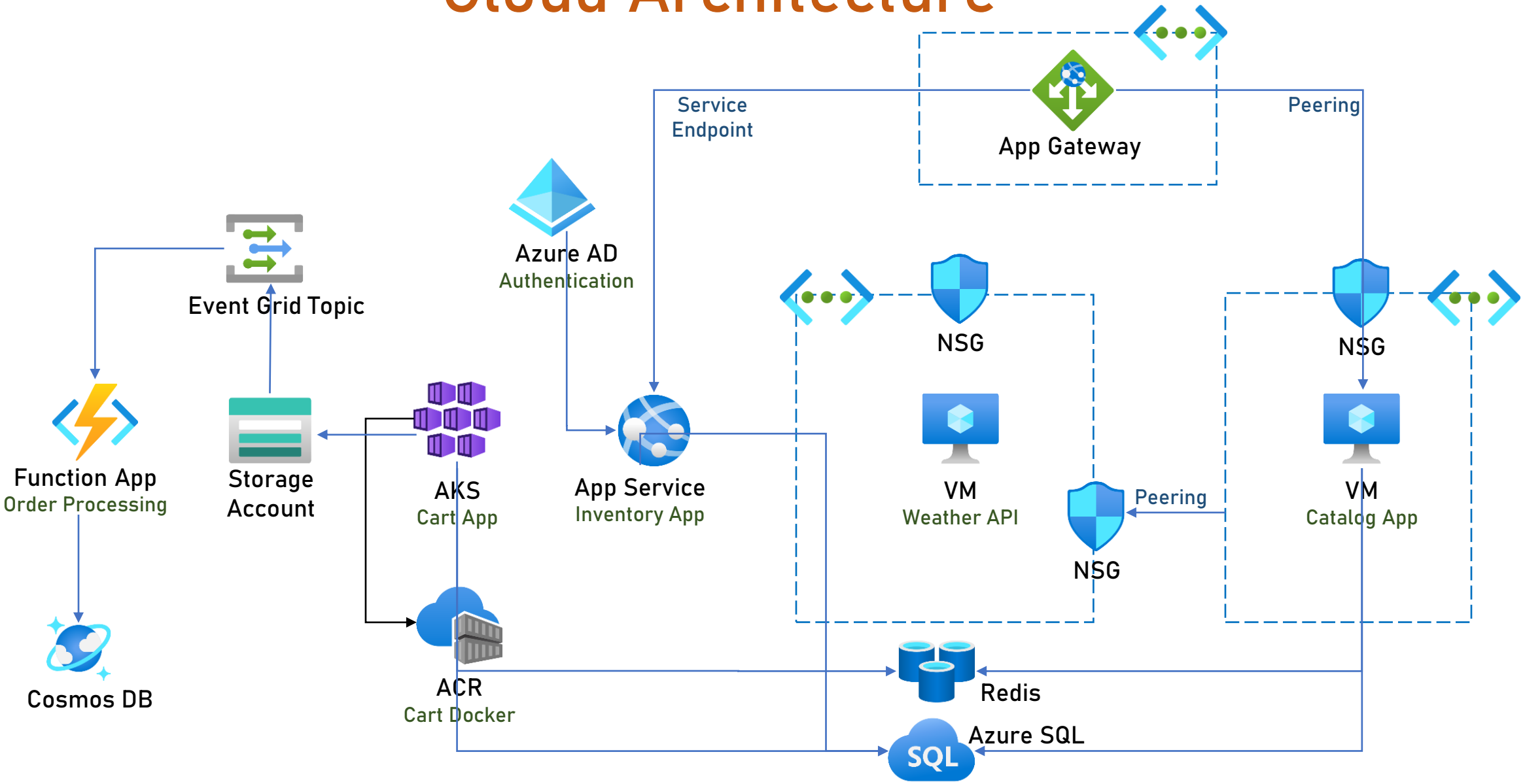
- MFA
- Conditional Access
- Audit Log
- Custom policies
- Custom pages
- And more…

Authentication Features

- Quite complex to set up
- A lot of moving parts
- We won't demonstrate it…

ReadIt!

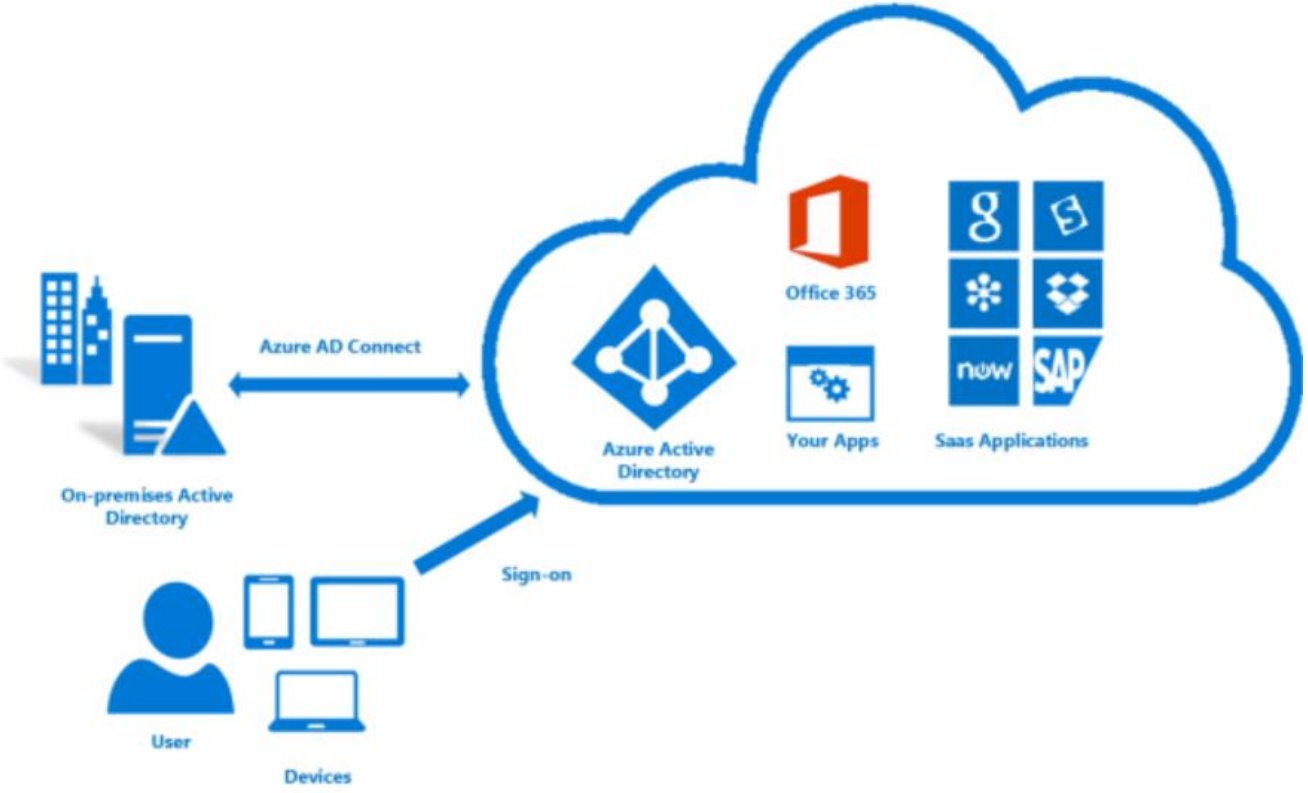
Cloud Architecture



Syncing Azure AD with On Prem

- Many organizations want to sync their on prem Active Directory with Azure AD
- Useful when the organization has apps on prem and in cloud and wants to have a single user base

AD Connect


Azure AD Connect
On-premises Active Directory
Azure Active Directory
Office 365
Your Apps
Saas Applications
Sign-on
User
Devices

Authentication with AD Connect

Password Hash Sync → The passwords are copied to Azure AD, Authentication happens in the cloud

Pass-Through → Passwords stay on-prem, Azure AD passes data to on-prem for validation

Monitoring in Azure

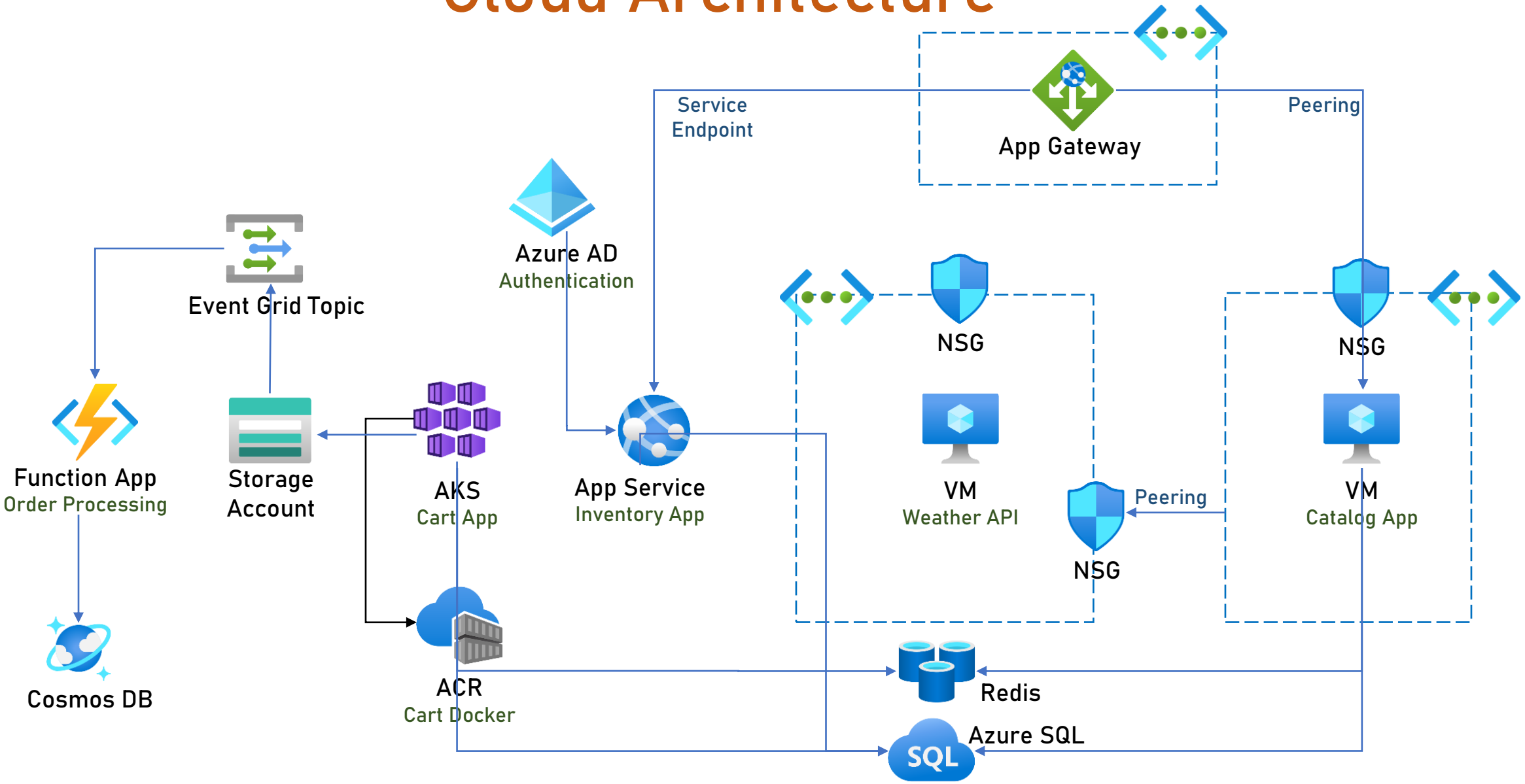
Memi Lavi
www.memilavi.com

Monitoring

- A working app is not enough
- We must know its status, how it performs, and when it has problems
- This is done via monitoring

ReadIt!

Cloud Architecture



Monitoring in Azure

- Azure offers a lot of built in monitoring mechanisms
- It's a good idea to be familiar with as many as possible
- Also – a centralized monitoring hub where all monitoring data is streamed, and can be queried, or used for triggers
- Extremely cost effective

Monitoring in Azure

- Monitoring is based on two types of data:

Metrics →

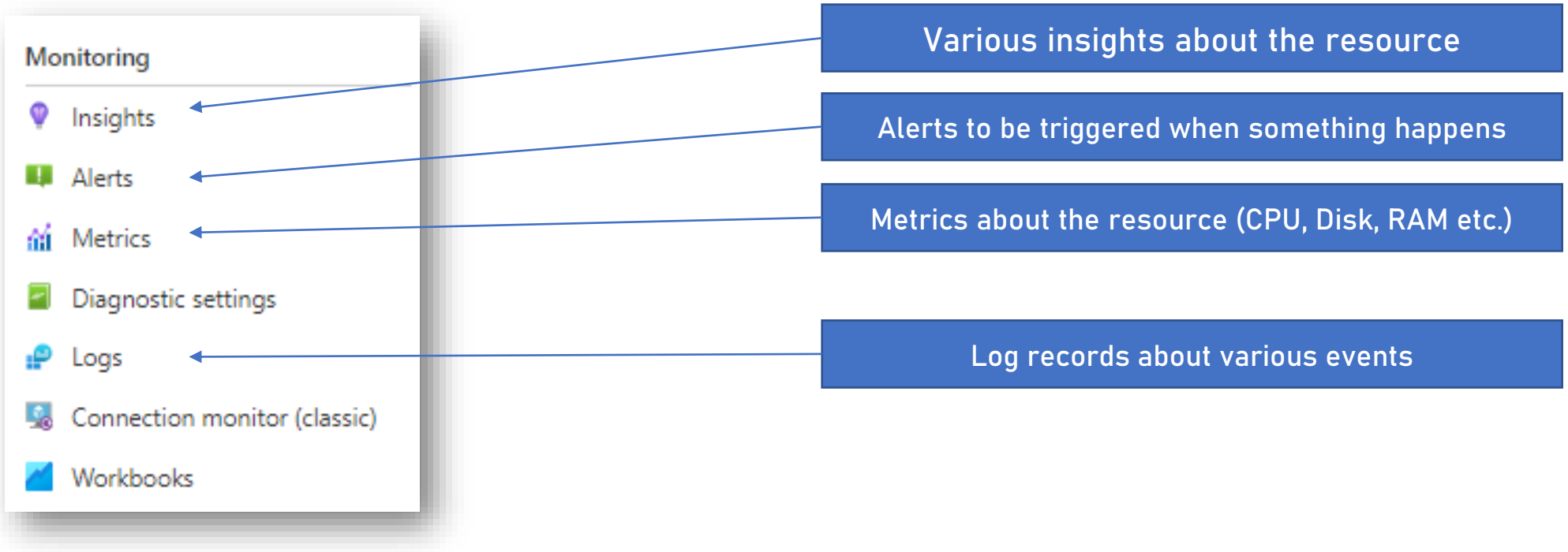
- Numeric values describing resource's aspect at a specific point in time
- Examples: CPU, Disk, Response Time

Logs →

- Events that occurred in the system
- Textual & numeric
- Examples: System started, Error occurred

Resource Monitoring

- Almost every resource in Azure has a “Monitoring” section



Alerts

- Get notifications about events in your resources
- Examples:
  - VM's CPU goes above 90%
  - More than 20% of requests fails
  - Server error occurs in the last hour

Alerts Components

Condition → When to trigger the alert (ie. CPU goes above 90%)

Actions → What to do? Usually – send notifications.
Notifications are sent to **Action Groups**.

Details → Contents of notification

Alerts Pricing

- Per metrics measured (0.10$ / metric)
- Per notification type
  - 1K email, 1K push notifications, 100K web hooks, 100 SMS in the US are included for free each month
- All in all – quite cost effective

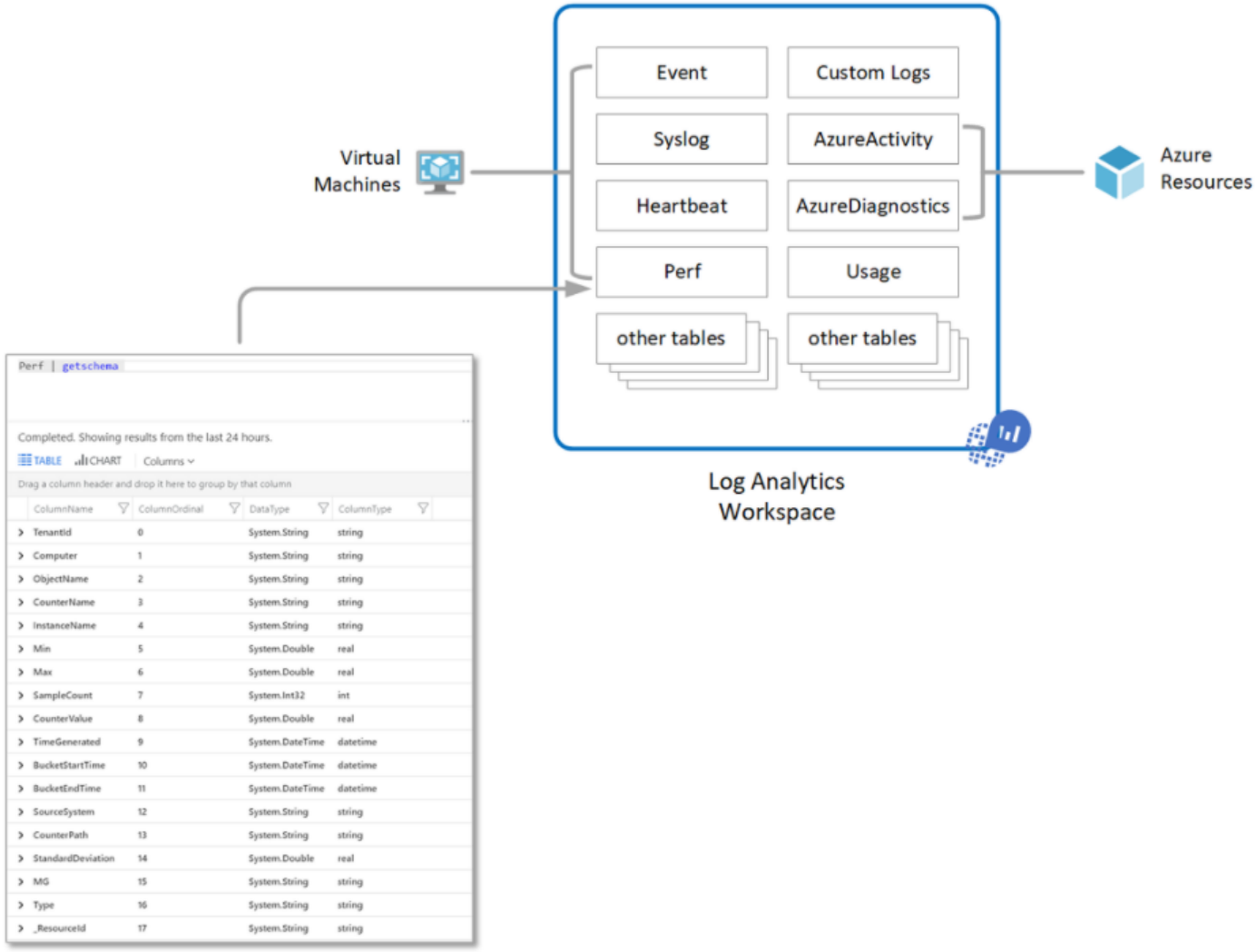
Logs & Analytics Workspace

- Almost every Azure resource generate logs
- Might contain data about performance, events, errors etc.
- Logs records need central repository to be stored and viewed
- This is the Log Analytics Workspace

Log Analytics Workspace

- A central location for storing, organizing and analyzing logs
- Aggregates logs from all connected, monitored resources
- Uses specialized query language to query logs
- Located in a designated region
- Better be the same region of the resources to save costs

Log Analytics Workspace




```
Perf | getschema
```

Completed. Showing results from the last 24 hours.

TABLE CHART Columns

Drag a column header and drop it here to group by that column

ColumnName	ColumnOrdinal	DataType	ColumnType
TenantId	0	System.String	string
Computer	1	System.String	string
ObjectName	2	System.String	string
CounterName	3	System.String	string
InstanceName	4	System.String	string
Min	5	System.Double	real
Max	6	System.Double	real
SampleCount	7	System.Int32	int
CounterValue	8	System.Double	real
TimeGenerated	9	System.DateTime	datetime
BucketStartTime	10	System.DateTime	datetime
BucketEndTime	11	System.DateTime	datetime
SourceSystem	12	System.String	string
CounterPath	13	System.String	string
StandardDeviation	14	System.Double	real
MG	15	System.String	string
Type	16	System.String	string
_ResourceId	17	System.String	string

Insights

- A collection of metrics, statistics and insights about the resource
- Specific to resource type
- Generated automatically
- Code-based services (App Services, apps on VMs) can integrate Application Insights into the code and gain a lot of data about app usage, performance, etc.

Azure Monitor

- A central location for all the monitoring aspects of Azure's resources
- Provides access to metrics, logs, insights and more
- Has additional capabilities not found in the individual resources

Resource Tags

- Resources are organized into Resource Groups
- Sometimes we want more information about resources:
  - Which environment? Test? Production?
  - To which app it belongs?
  - Which group is responsible for it?

Resource Tags

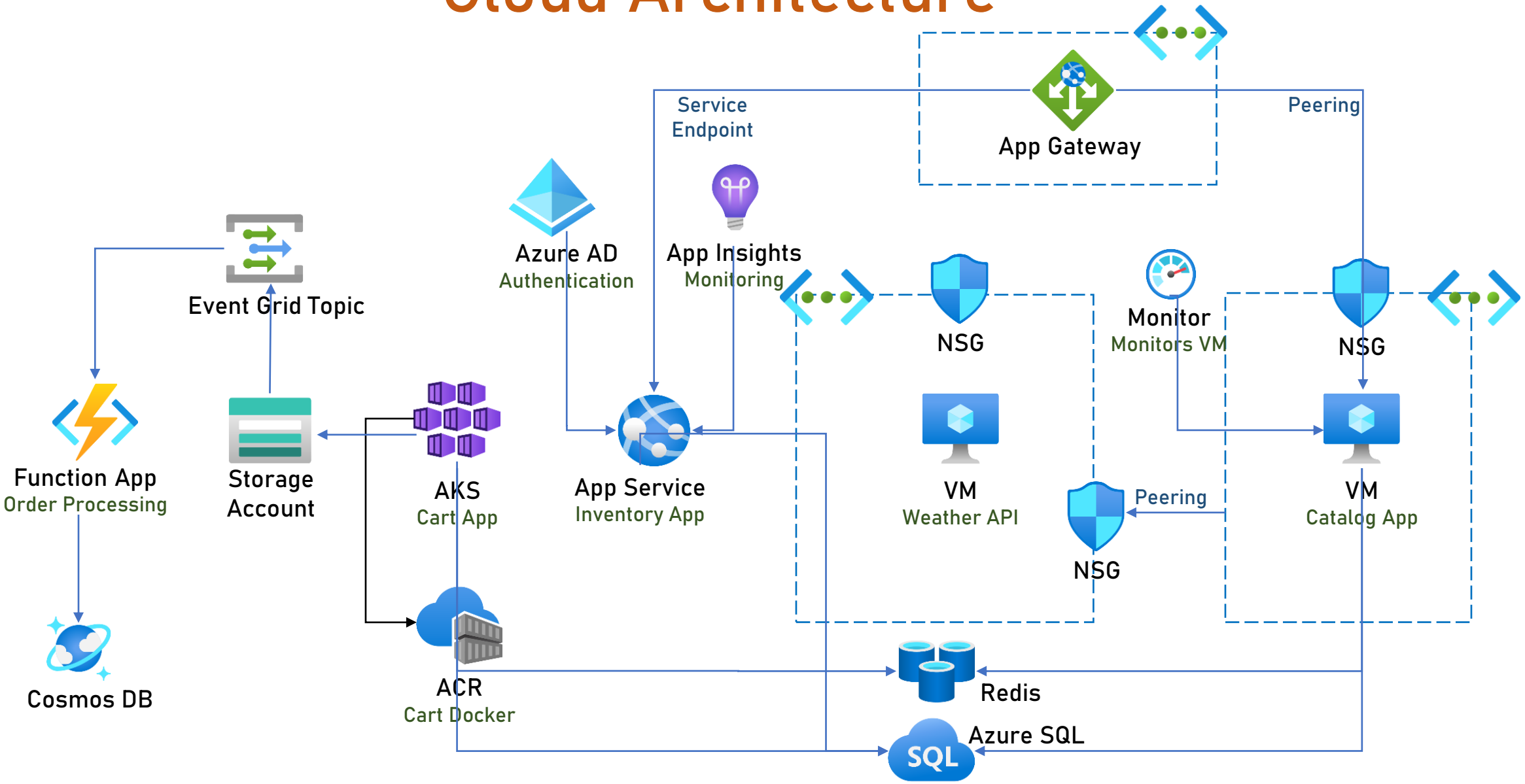
- For this we have Resource Tags
- Tags help organize resources using name-value pairs
- Examples:
  - Environment: Test
  - App: readit
  - Group: the-A-team

Resource Tags

- Can be set during creation of resource or after that
- Useful for many scenarios:
  - Resource querying (show all resource of the A team)
  - Cost analysis (how much did the test environment cost last month?)
  - And more…

ReadIt!

Cloud Architecture



Security in Azure

Memi Lavi
www.memilavi.com

Security

- Security is one of the most important parts of every system
- Azure offers a lot of security measures for its resources
- It's extremely important to use those measures and follow security patterns to avoid security incidents
- We've covered most of them, here we'll summarize and emphasize some new techniques

VM Security Best Practices

- Restrict access to the VM as much as possible
- Make sure only the required ports are open to the internet (22/1389/443/80)
- Limit access to specific IP addresses when possible

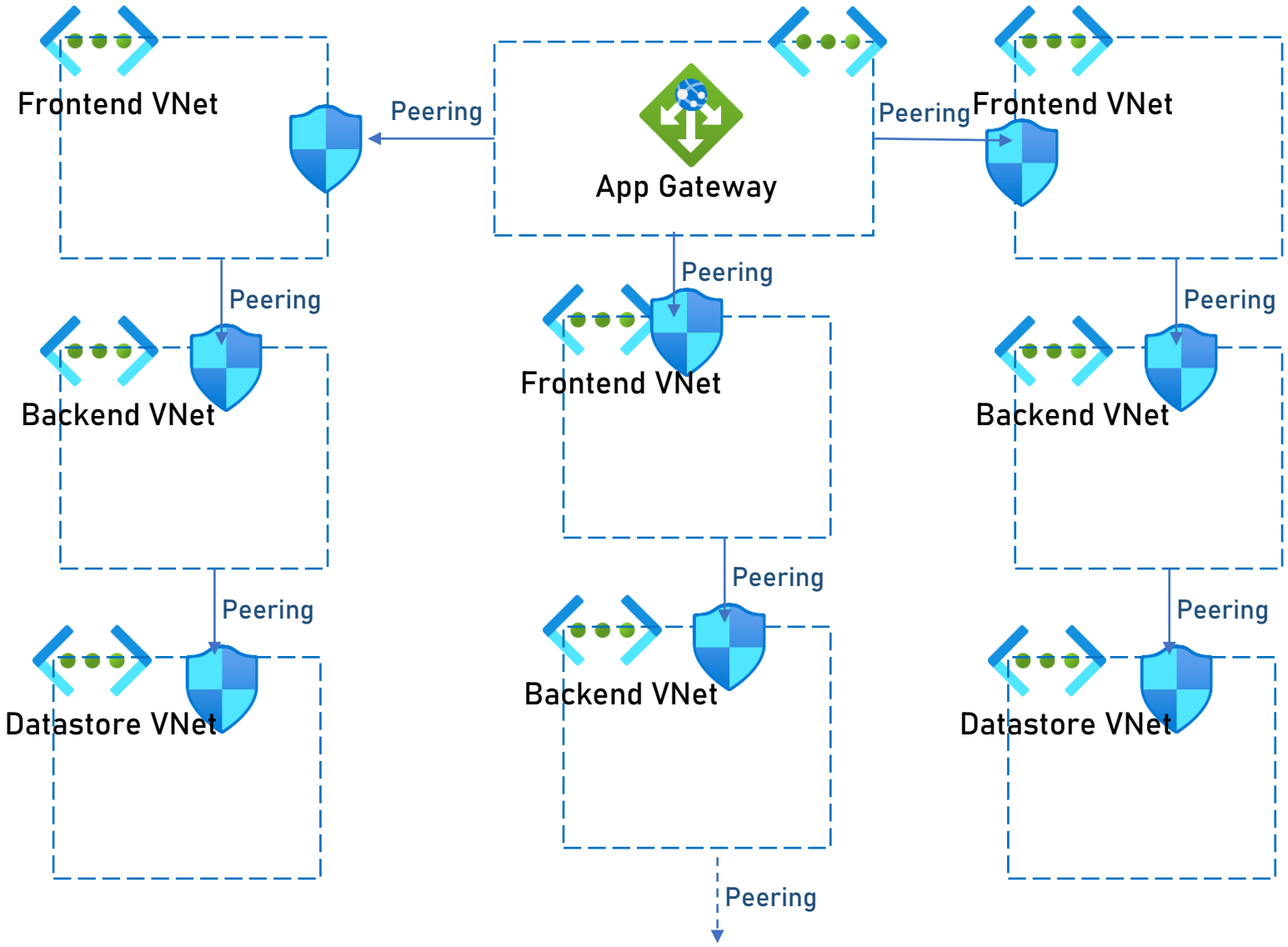
VM Security Best Practices

- Prefer using Bastion for accessing the VM, so no need for open ports
- If the VM is not public facing – place it in a VNet that's not connected directly to the internet

Networking Security Best Practices

- VNet that contains private resources only – should not be exposed to the internet
- ALWAYS use NSG to restrict access to subnets
- Use Service Endpoints / Private Endpoint to restrict access to resources
- Use the Hub-and-Spoke security model

Hub and Spoke



Database Security Best Practices

- Use encryption at rest and encryption at transit (usually On by default)
- Connect DB to relevant VNet using Services Endpoint / Private Endpoint
- Access DB from app using Managed Identities
- Use DB's Firewall rule to restrict external access

App Service Security Best Practices

- Don't expose directly to the internet, use Application Gateway
- Connect to App Gateway's VNet using Service Endpoint / Private Endpoint
- Use Azure AD for Authentication, enforce with MFA
- Use Managed Identity to access other resources when possible

KeyVault

- Many apps have secrets that need to be kept safely
  - Connection Strings
  - Keys
  - Certificates
  - API Keys
  - And more…

KeyVault

- Usually kept in configuration files, configuration DB etc.
- Not really secure…
- KeyVault solves this problem

KeyVault

- Safely stores secrets of various types
- Very restricted access – needs Azure AD authentication
- Supports Hardware Security Modules (for enhanced security)
- Easily manageable
- Accessed via REST API

KeyVault

- Very cost effective

Key Vault

REGION:

West Europe

Vaults

Operations (Standard or Premium)

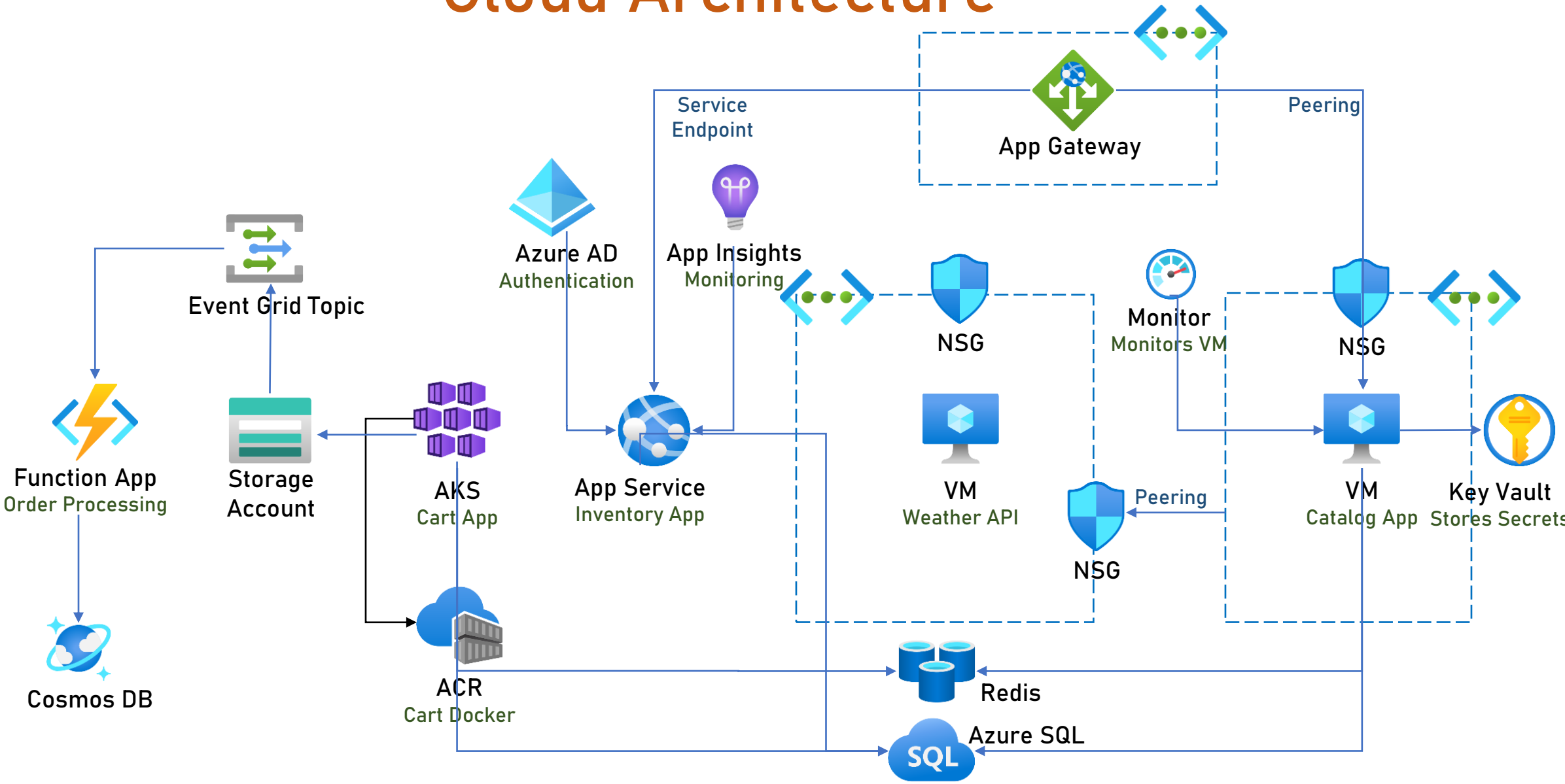
1000000	×	$0.030	=	$3.00
Operations		Per 10000 operations		

Microsoft Defender for Cloud

- A central location for monitoring and alerting security-related issues
- Displays a summarized list of problems found in the subscription's resources
- In some cases, allow a single-click fix
- Good practice to take a look once in a while

ReadIt!

Cloud Architecture



DR in Azure

Memi Lavi
www.memilavi.com

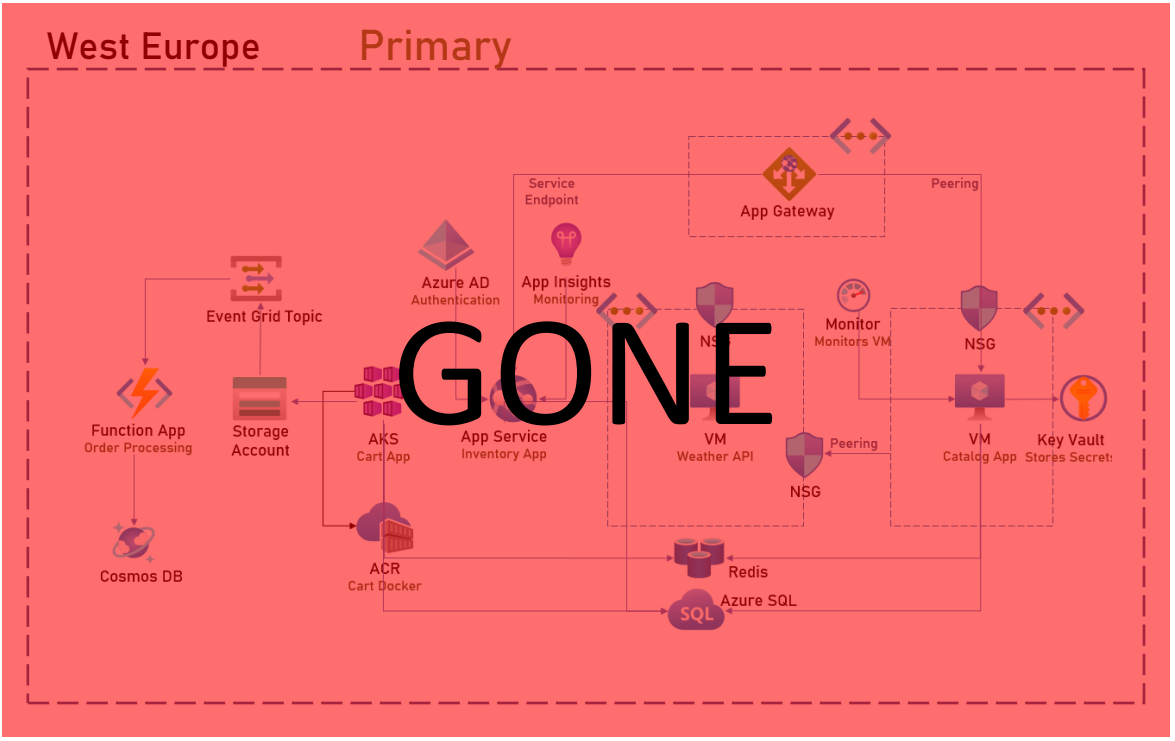
DR

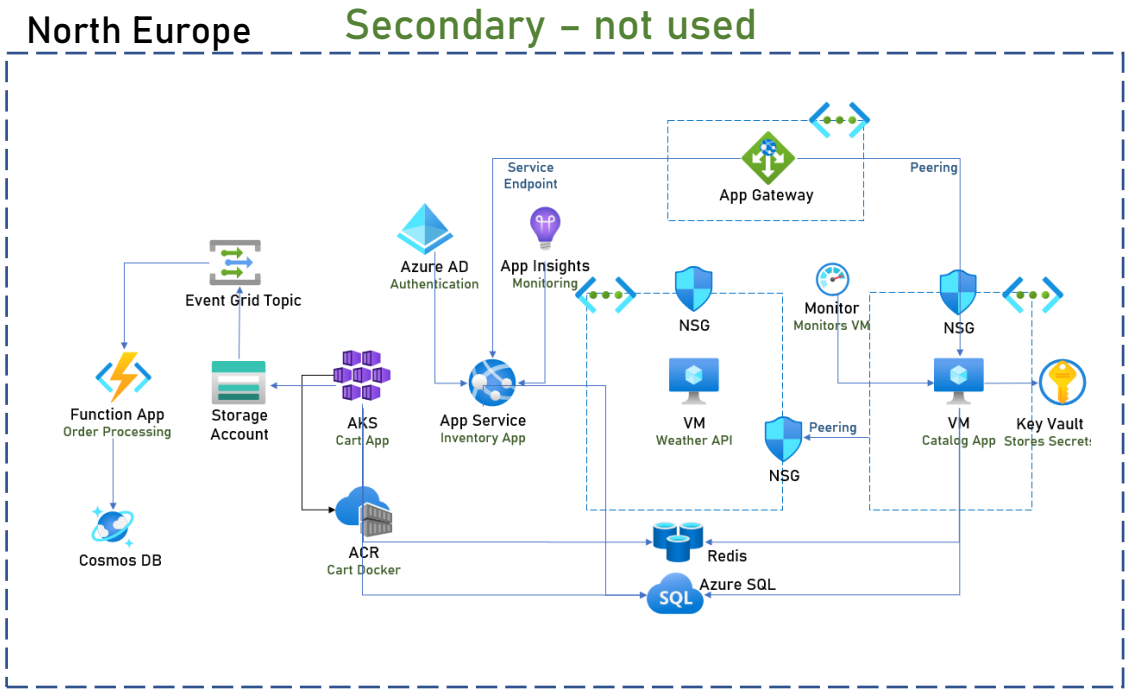
- Disaster Recovery
- A plan to recover from a complete shutdown of a Region
  - Usually as a result of a disaster (earthquake, flood, etc)
- Some apps require it, some don't
- Might have substantial cost aspects
- Remember: A complete shutdown of a Region is extremely rare

How DR Works?

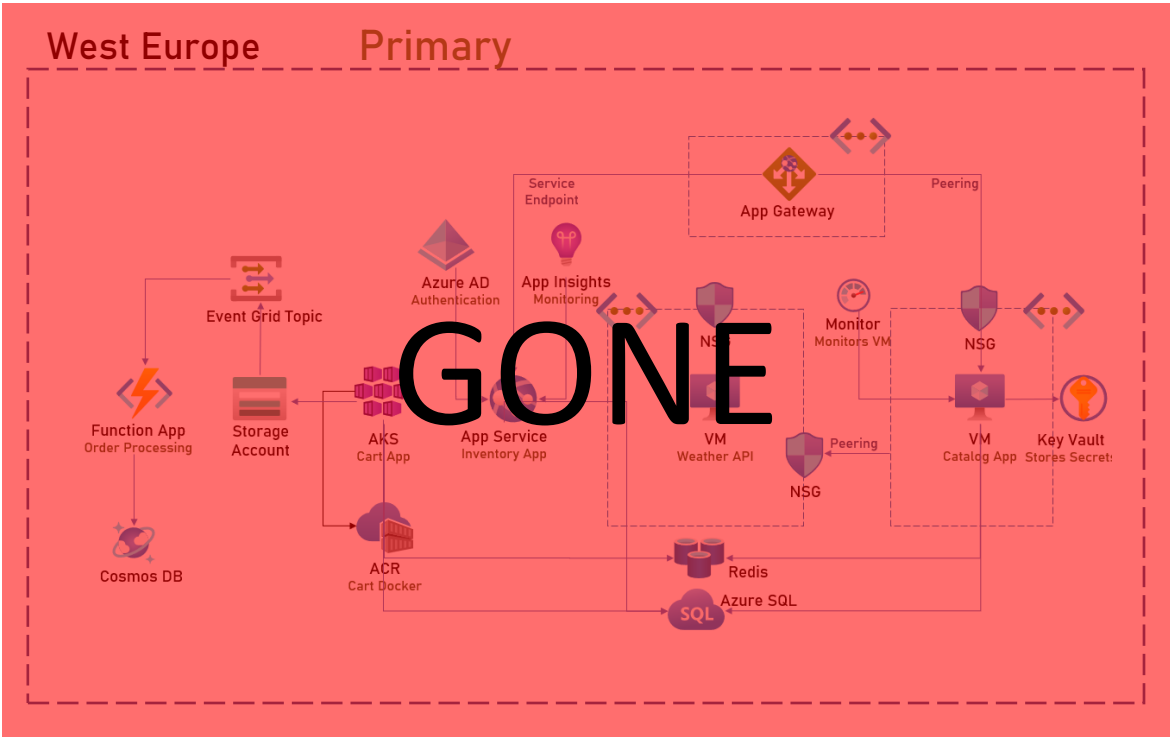
- In order to set up DR, we need to do the following:
  - Select a DR site
    - A secondary Region that will function as our primary in case of a disaster
    - Configure it to be ready for activation when necessary

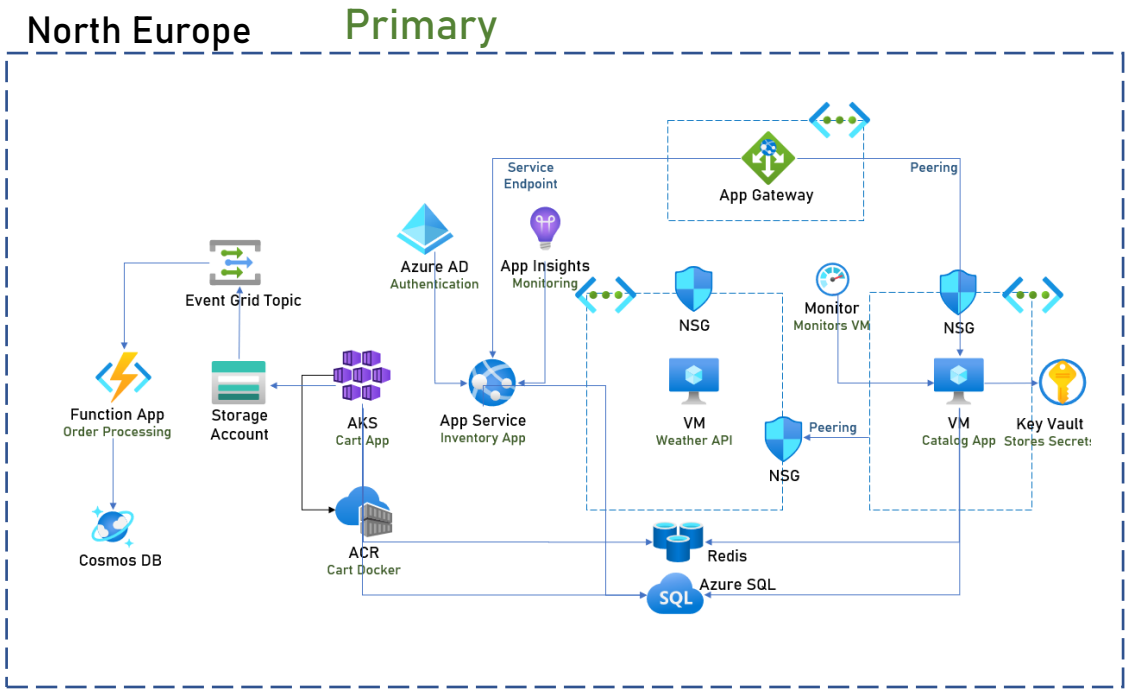
How DR Works?


West Europe
Primary
GONE
Service Endpoint
App Gateway
Peering
Azure AD
Authentication
App Insights
Monitoring
Event Grid Topic
Monitor
Monitors VM
NSG
Function App
Order Processing
Storage Account
AKS
Cart App
App Service
Inventory App
VM
Weather API
Peering
VM
Catalog App
Key Vault
Stores Secrets
NSG
Cosmos DB
ACR
Cart Docker
Redis
Azure SQL
SQL


North Europe
Secondary – not used
Service Endpoint
App Gateway
Peering
Azure AD
Authentication
App Insights
Monitoring
Event Grid Topic
NSG
Monitor
Monitors VM
NSG
Function App
Order Processing
Storage Account
AKS
Cart App
App Service
Inventory App
VM
Weather API
Peering
VM
Catalog App
Key Vault
Stores Secrets
NSG
Cosmos DB
ACR
Cart Docker
Redis
Azure SQL
SQL

How DR Works?


West Europe
Primary
GONE
Service Endpoint
App Gateway
Peering
Azure AD
Authentication
App Insights
Monitoring
Event Grid Topic
Monitor
Monitors VM
NSG
Function App
Order Processing
Storage Account
AKS
Cart App
App Service
Inventory App
VM
Weather API
Peering
VM
Catalog App
Key Vault
Stores Secrets
NSG
Cosmos DB
ACR
Cart Docker
Redis
Azure SQL
SQL


North Europe
Primary
Service Endpoint
App Gateway
Peering
Azure AD
Authentication
App Insights
Monitoring
Event Grid Topic
NSG
Monitor
Monitors VM
NSG
Function App
Order Processing
Storage Account
AKS
Cart App
App Service
Inventory App
VM
Weather API
Peering
VM
Catalog App
Key Vault
Stores Secrets
NSG
Cosmos DB
ACR
Cart Docker
Redis
Azure SQL
SQL

DR Concepts

- Hot / Cold

Hot →

- Failover to secondary site happens automatically with no downtime
- No data loss
- Requires duplicate infrastructure
- The most expensive method

Cold →

- Failover to secondary site takes some time
- Might be manual
- Some data might be lost
- Less expensive

DR Concepts

- Hot or Cold – how to decide?
- Depends on the system's requirements
- A global ecommerce website, serving million of customers – probably Hot
- An HR app for the organization – definitely Cold (if at all…)

DR Concepts

- RPO / RTO

RPO →

- Recovery Point Objective
- How much data we allow ourselves to lose in case of a disaster
- Usually measured in minutes
- In other words – what's the frequency of data sync to the secondary region
- Example: We have an RPO of 5 minutes

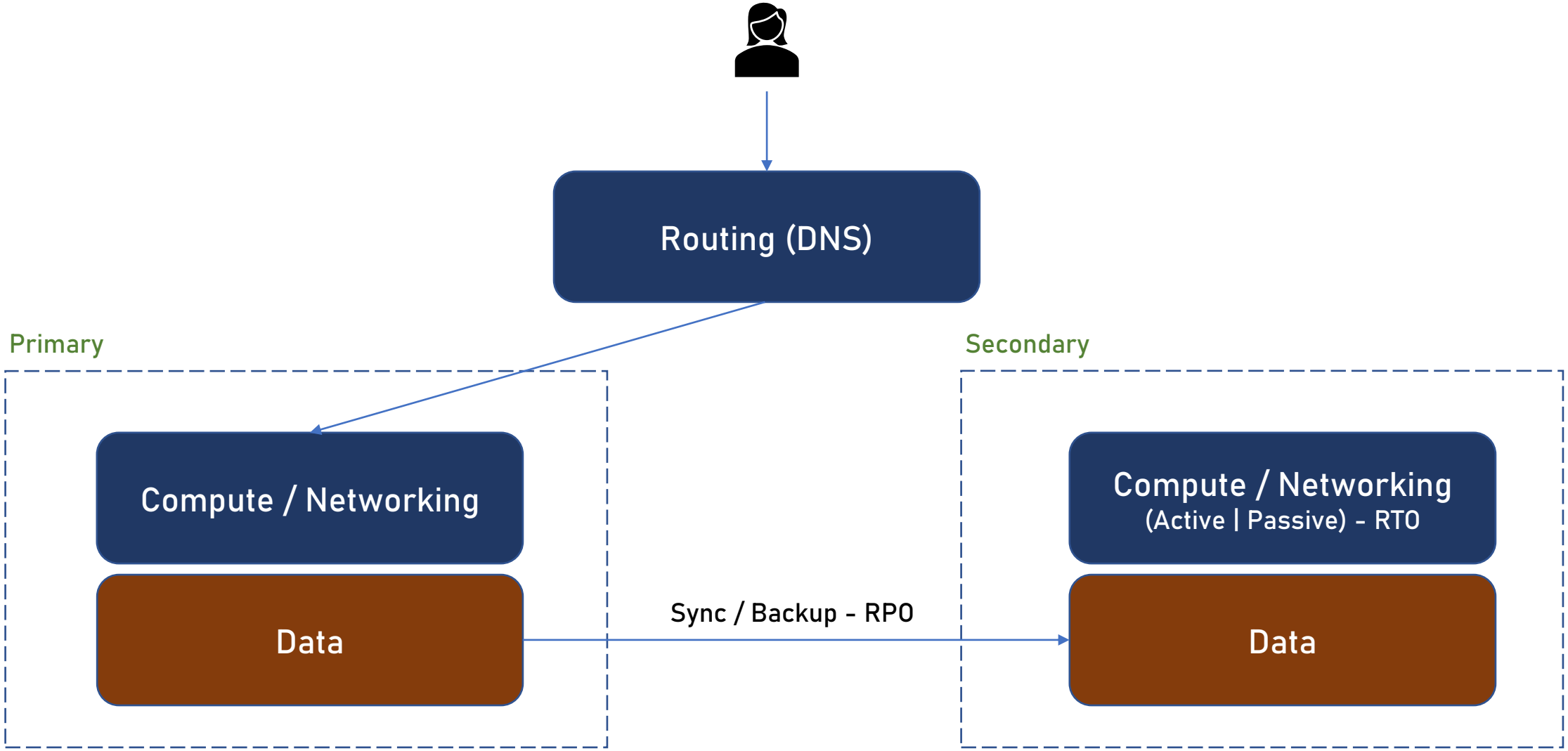
RTO →

- Recovery Time Objective
- How much downtime we can tolerate in case of a disaster
- Usually measured in minutes
- In other words – how long it should take before the system is up again
- Not necessarily with the most up to date data, depends on the RPO

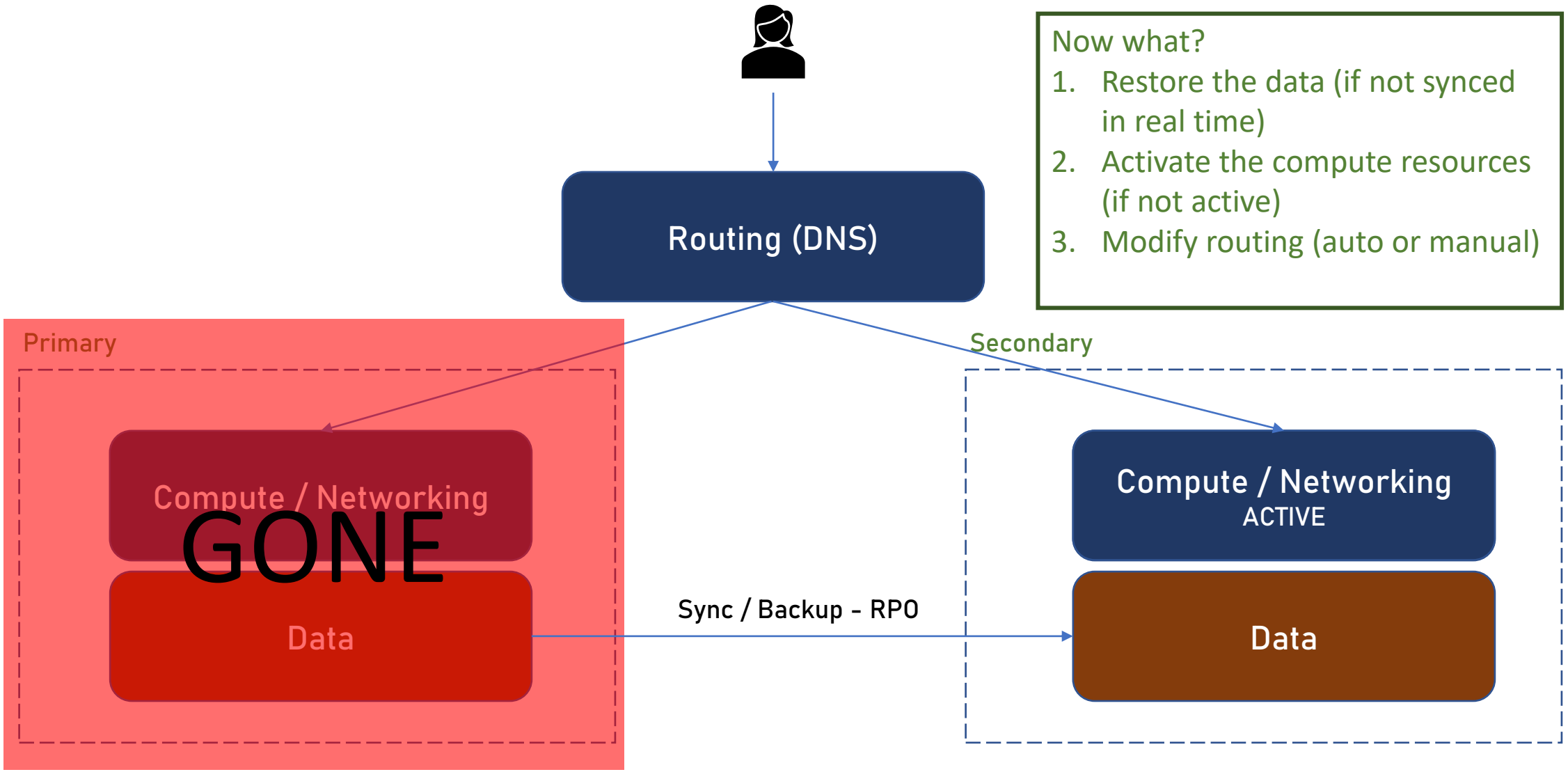
DR Concepts

- RPO and RTO– how to decide?
- Depends on the system's requirements
- A massive reporting system will probably go for low RPO, but can compromise on the RTO
- A global chat will focus on RTO

Basics of DR Implementation



Basics of DR Implementation



Now what?

1. Restore the data (if not synced in real time)
2. Activate the compute resources (if not active)
3. Modify routing (auto or manual)

DR of Data in Azure

- Main question when designing the DR of data is:

What is the RPO?

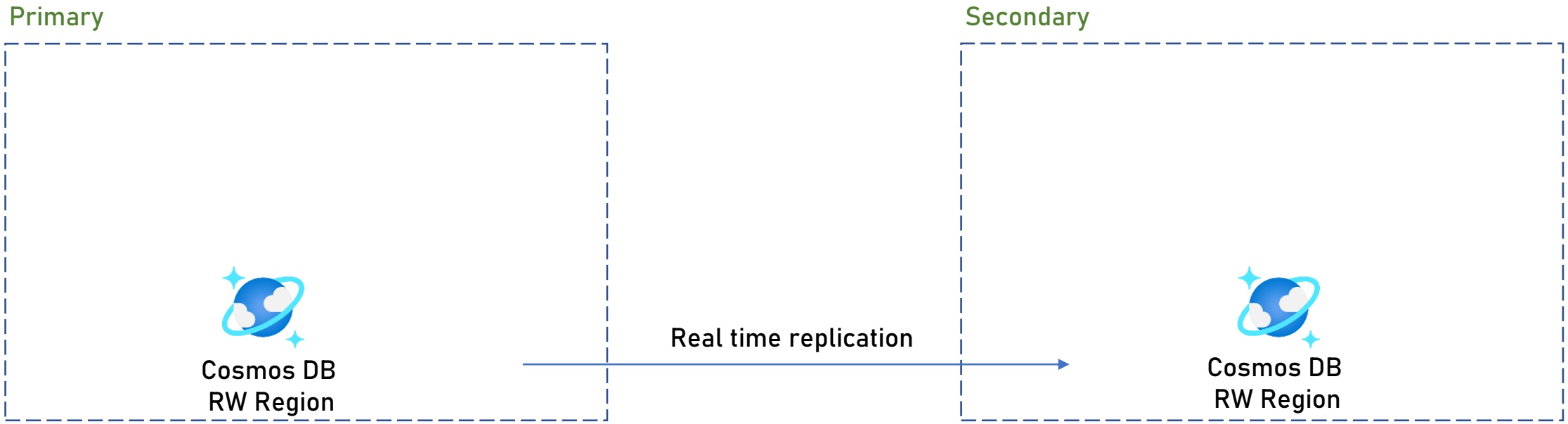
(Or – how much data loss do we tolerate?)

DR of Data in Azure

- If RPO = 0 (no data loss in case of disaster):
  - We need database that always syncs with the secondary region
  - Currently – three such databases in Azure:
    - Azure SQL (with Geo-Replication and Failover Group)
    - Cosmos DB (with multi-region account)
    - Azure Storage (with GRS redundancy)

DR of Data in Azure

RPO = 0

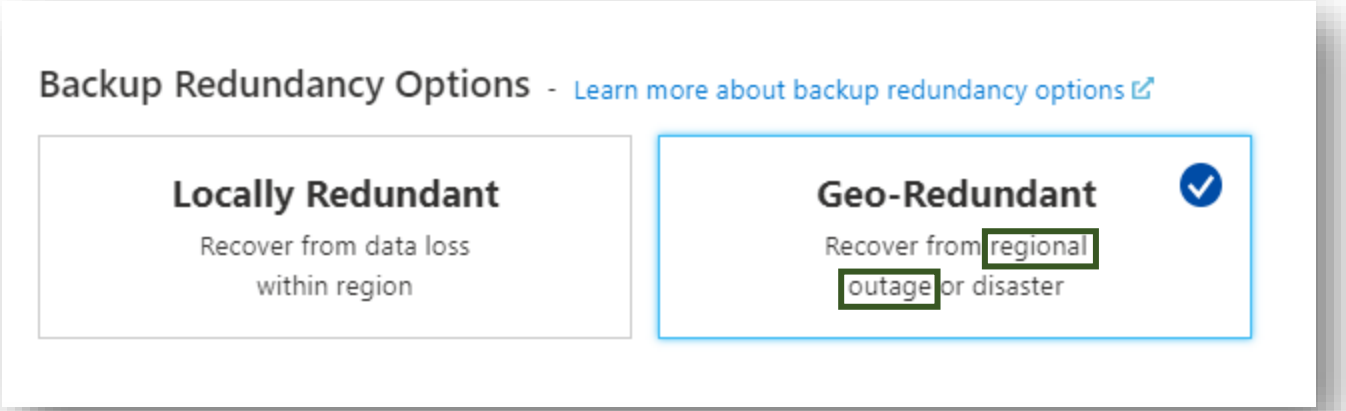


DR of Data in Azure

- If RPO > 0 (some data can be lost):
  - Ensure DB's backup frequency is compliant with the RPO
  - The backup storage should be GRS

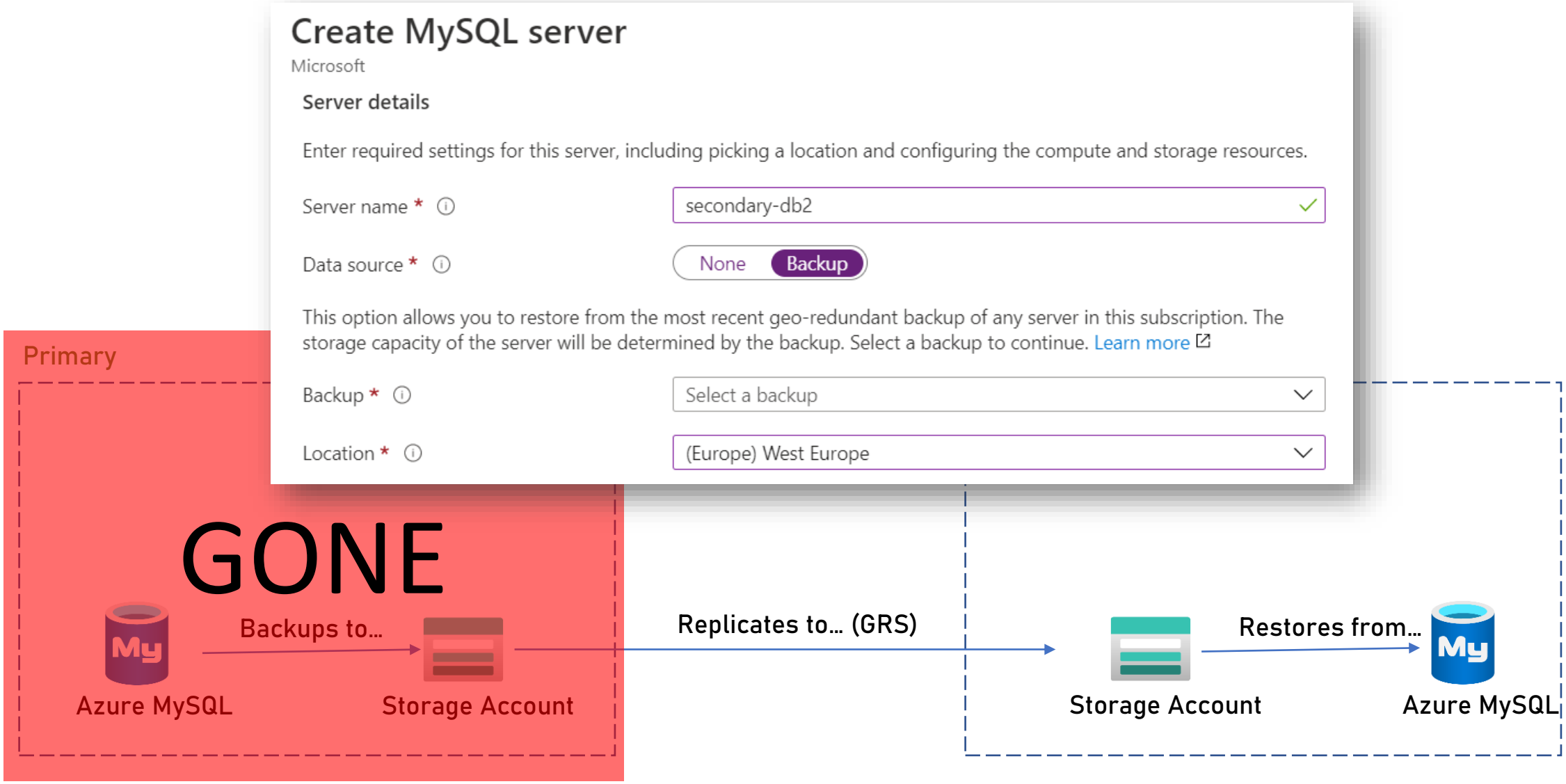
DR of Data in Azure

- Example – Azure MySQL:



The General purpose storage is the backend storage supporting General Purpose and Memory Optimized tier server. For servers with general purpose storage up to 4 TB, full backups occur once every week. Differential backups occur twice a day. Transaction log backups occur every five minutes. The backups on general purpose storage up to 4-TB storage are not snapshot-based and consumes IO bandwidth at the time of backup. For large databases (> 1 TB) on 4-TB storage, we recommend you consider

DR of Data in Azure



DR of Data in Azure

- Note that:
  - The RPO in the previous example is minimum 5 minutes (the backup frequency)
  - The second example is much cheaper, no secondary active database is needed when primary is active

DR of Compute in Azure

- Main question when designing the DR of compute is:

What is the RTO?

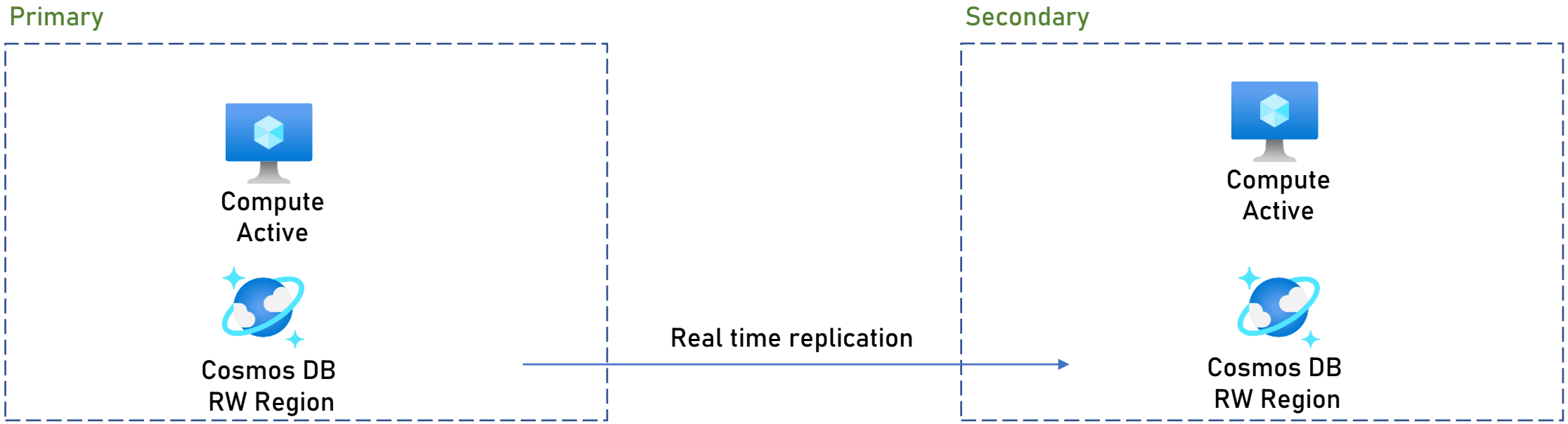
(Or – how much downtime can we tolerate?)

DR of Compute in Azure

- If RTO = 0 (no downtime in case of disaster):
  - Compute in secondary region should always be up and running

DR of Compute in Azure

RTO = 0

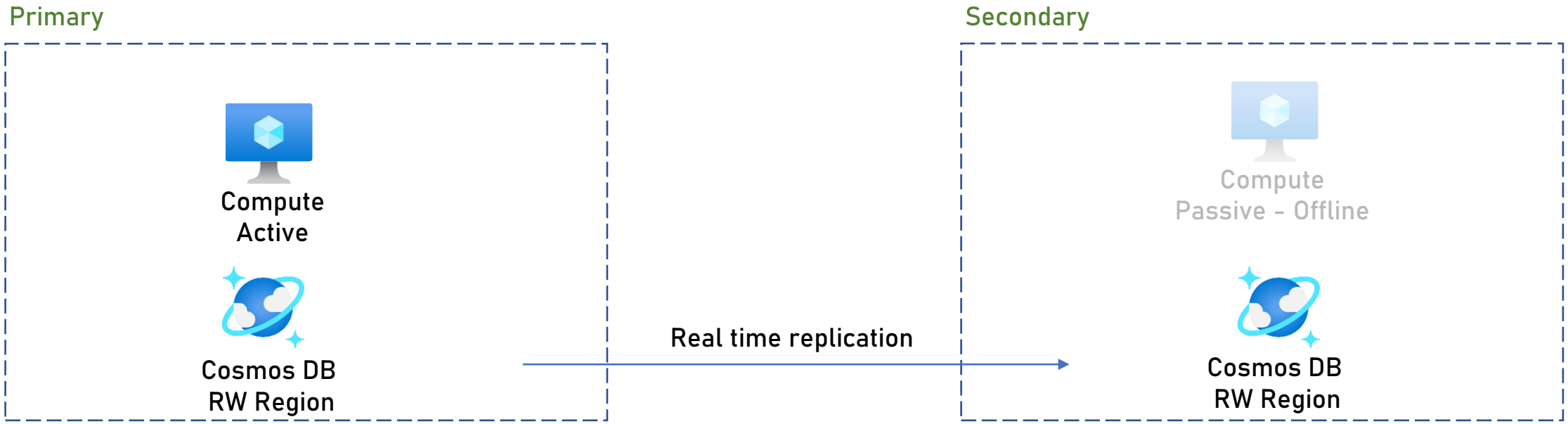


DR of Compute in Azure

- If RTO > 0 (some downtime is tolerated):
  - Either:
    - Have non-active (passive) compute on standby in secondary region
    - Create the compute when disaster occurs in secondary region

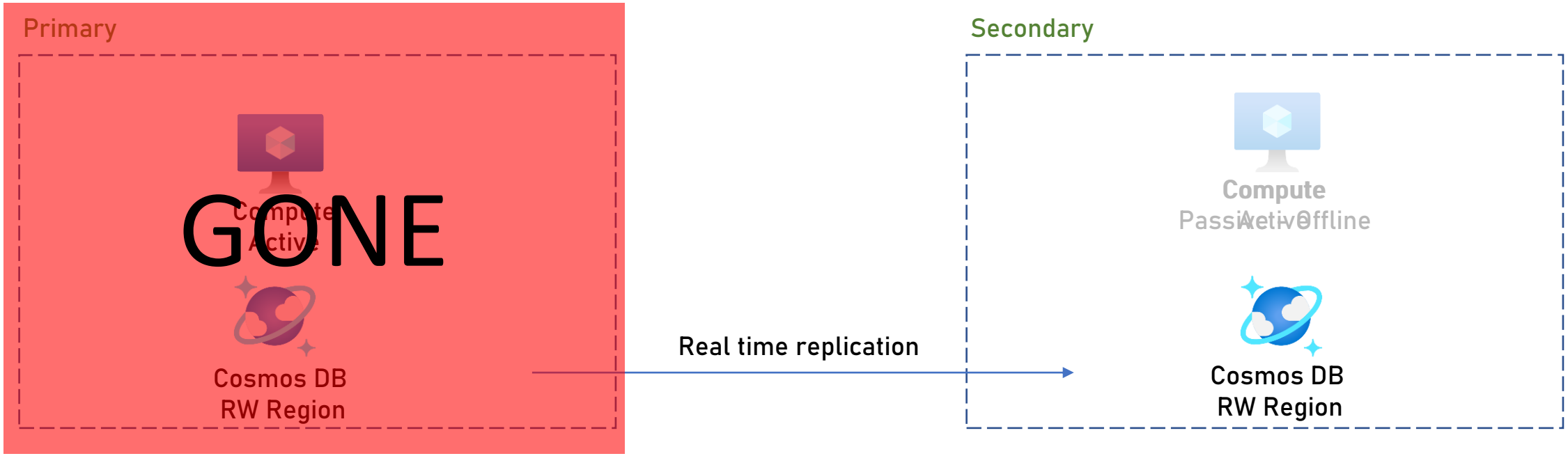
DR of Compute in Azure

RTO > 0



DR of Compute in Azure

RTO > 0



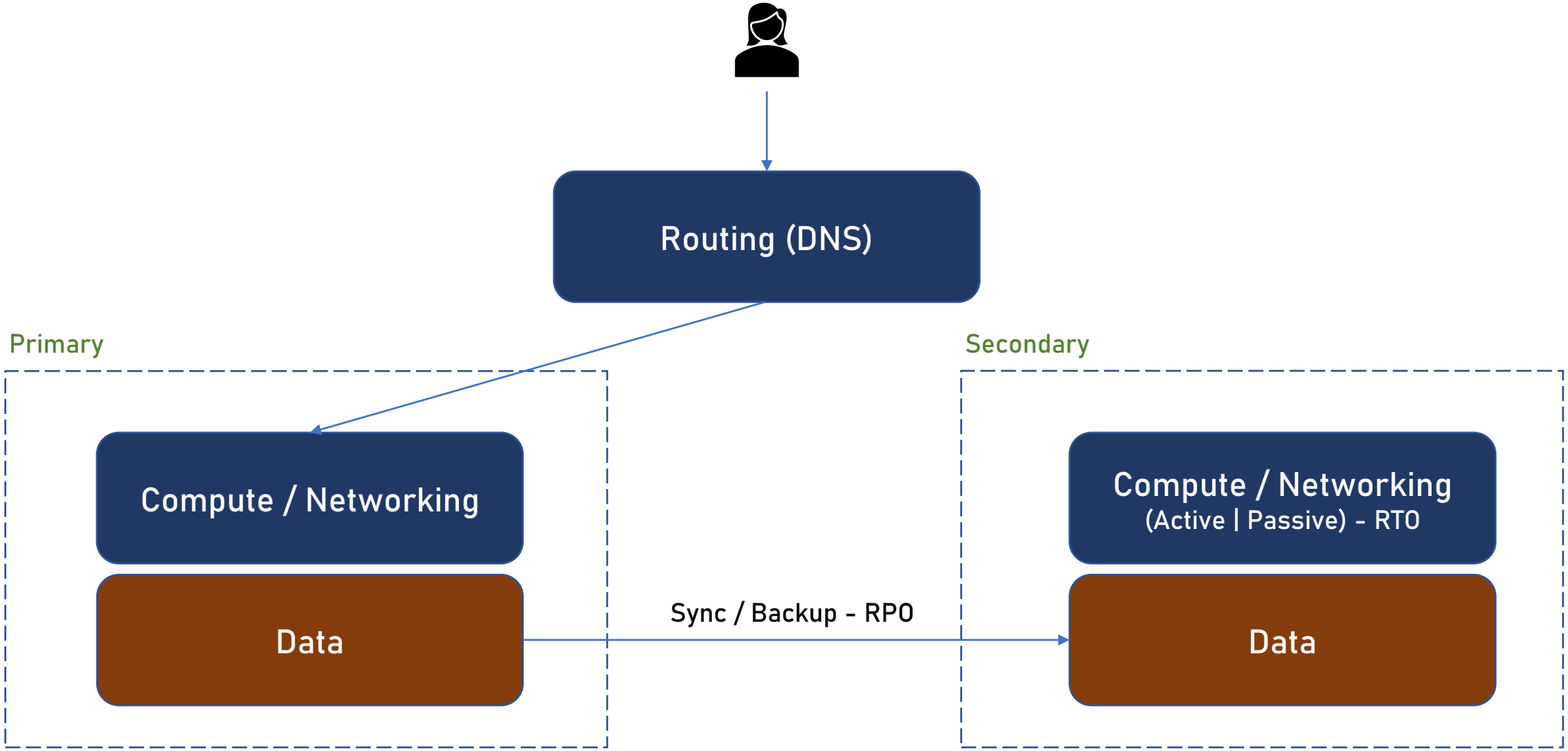
DR of Compute in Azure

- Note that:
  - The second example is much cheaper, no secondary active compute is needed when primary is active

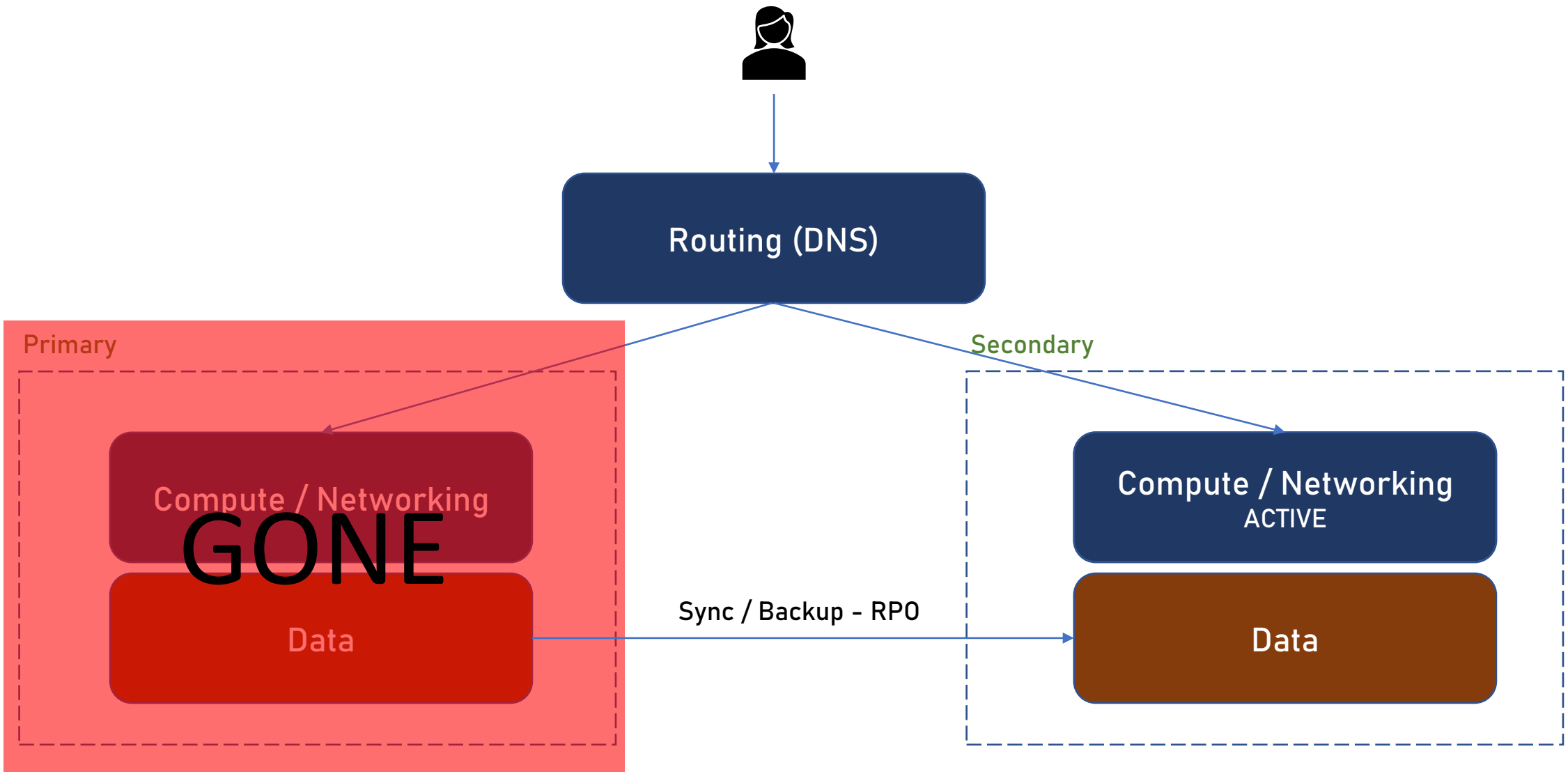
Routing in DR

- During DR users should be routed to the secondary region

Basics of DR Implementation



Basics of DR Implementation



Routing in DR

- Major three methods:
  - Inform the users about the new address of the app (in the secondary region)
  - Manually change DNS record to point to the secondary region
  - Use automatic routing

Routing in DR

- Azure has two automatic routing services

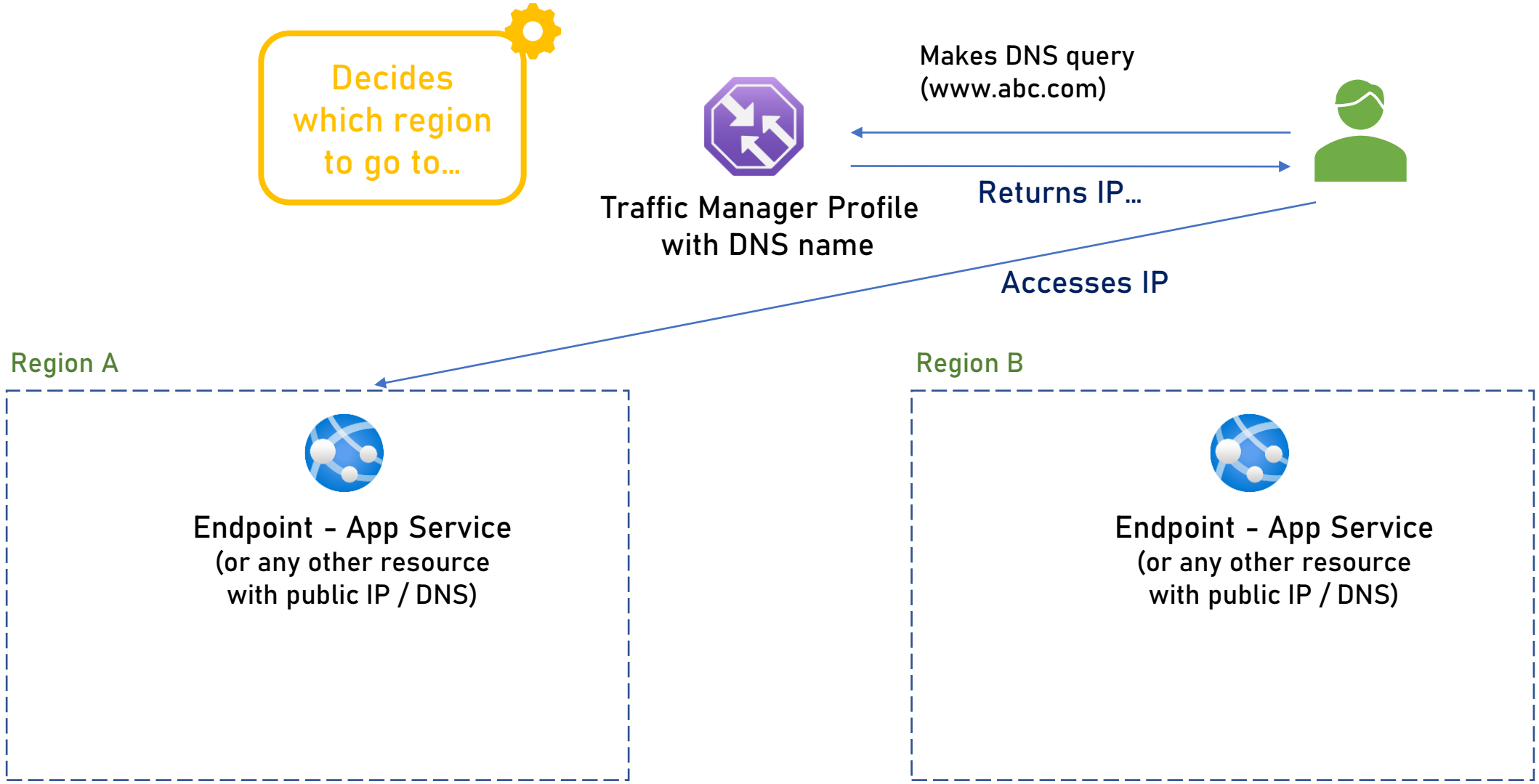
Traffic Manager

Front Door

Azure Traffic Manager

- DNS-based traffic load balancer
- Enables traffic distribution across global Azure regions
- Provides high availability and responsiveness

How Does Azure Traffic Manager Work?



Routing Algorithms

Priority	Always use primary service, when it's down – using backup endpoints (That's the DR…)
Weighted	Distribute traffic across endpoints according to weights defined by you
Performance	Use the closest region to improve latency
Geographic	Direct traffic to specific geography based on the location of the DNS query
Multivalue	Returns list of healthy endpoints so the client can choose what to do with them
Subnet	Map source IP to endpoint

Traffic Manager Pricing

Traffic Manager

REGION:

West Europe

DNS Queries

10 Million/month = $5.40

Health Checks

Azure

2 Endpoints × $0.36 Per month = $0.72

Fast Interval Health Checks Add-on (Azure)

0 Endpoints × $1.00 Per month = $0.00

Fast endpoint health checks need to be purchased as an add-on to basic endpoint health checks.

External

0 Endpoints × $0.54 Per month = $0.00

Fast Interval Health Checks Add-on (External)

0 Endpoints × $2.00 Per month = $0.00

Fast endpoint health checks need to be purchased as an add-on to basic endpoint health checks.

Real User Measurements

0 Million measurements × $2.00 Per month = $0.00

Azure Front Door

- Global entry point for web apps
- Works on Layer 7 (HTTP/HTTPS)
- Multiple routing methods
- Similar to Application Gateway but in global scale

Azure Front Door Features

- URL-path based routing
- Session affinity
- SSL Offloading
- Web Application Firewall (WAF) integration
- URL Rewrites
- HTTP/2 support

Azure Front Door Pricing

Azure Front Door

REGION:

West Europe

Outbound Data Transfer

Zone 1: North America, Europe and Africa

100 GB	=	$17.00

Inbound Data Transfer

20 GB	=	$0.20

Routing rules

1 Rules	×	730 Hours	=	$21.90

Web Application Firewall (WAF)

Policy

0 Policies	×	$5.00 Per policy per month	=	$0.00

Custom Rules

0 Rules	×	$1.00 Per rule per month	=	$0.00
2 Requests processed (in millions)	×	$0.60 Per million requests	=	$1.20

Managed Ruleset

0 Default Rulesets	×	$20.00 Per ruleset per month	=	$0.00
1 Requests processed (in millions)	×	$1.00 Per million requests	=	$1.00

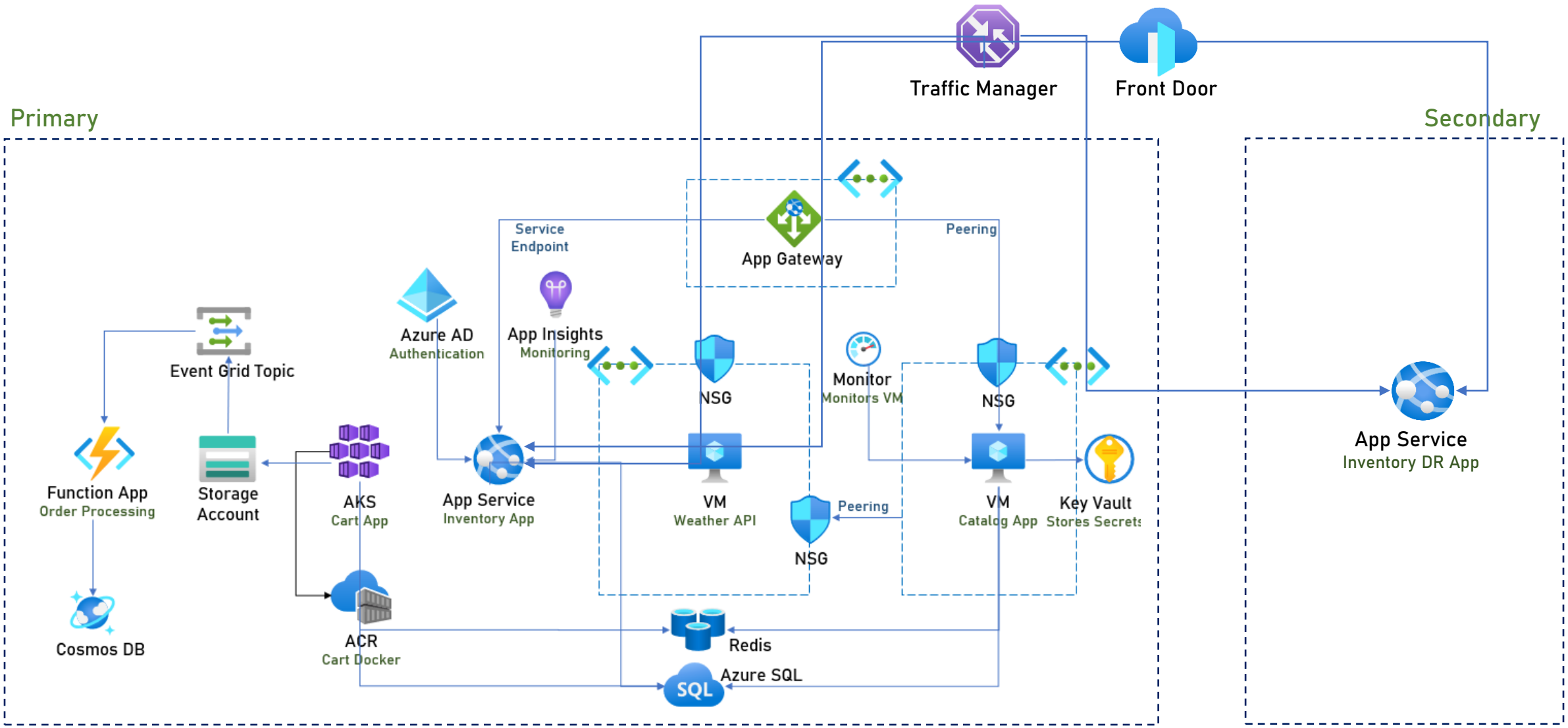
Upfront cost	$0.00
Monthly cost	$41.30

Traffic Manager vs Front Door

- Which one to choose?
- Generally – if you need HTTP-related capabilities go with Front Door
- Examples:
  - URL-path based routing
  - SSL Offloading
  - Web Application Firewall
- Otherwise – go with Traffic Manager, usually cheaper

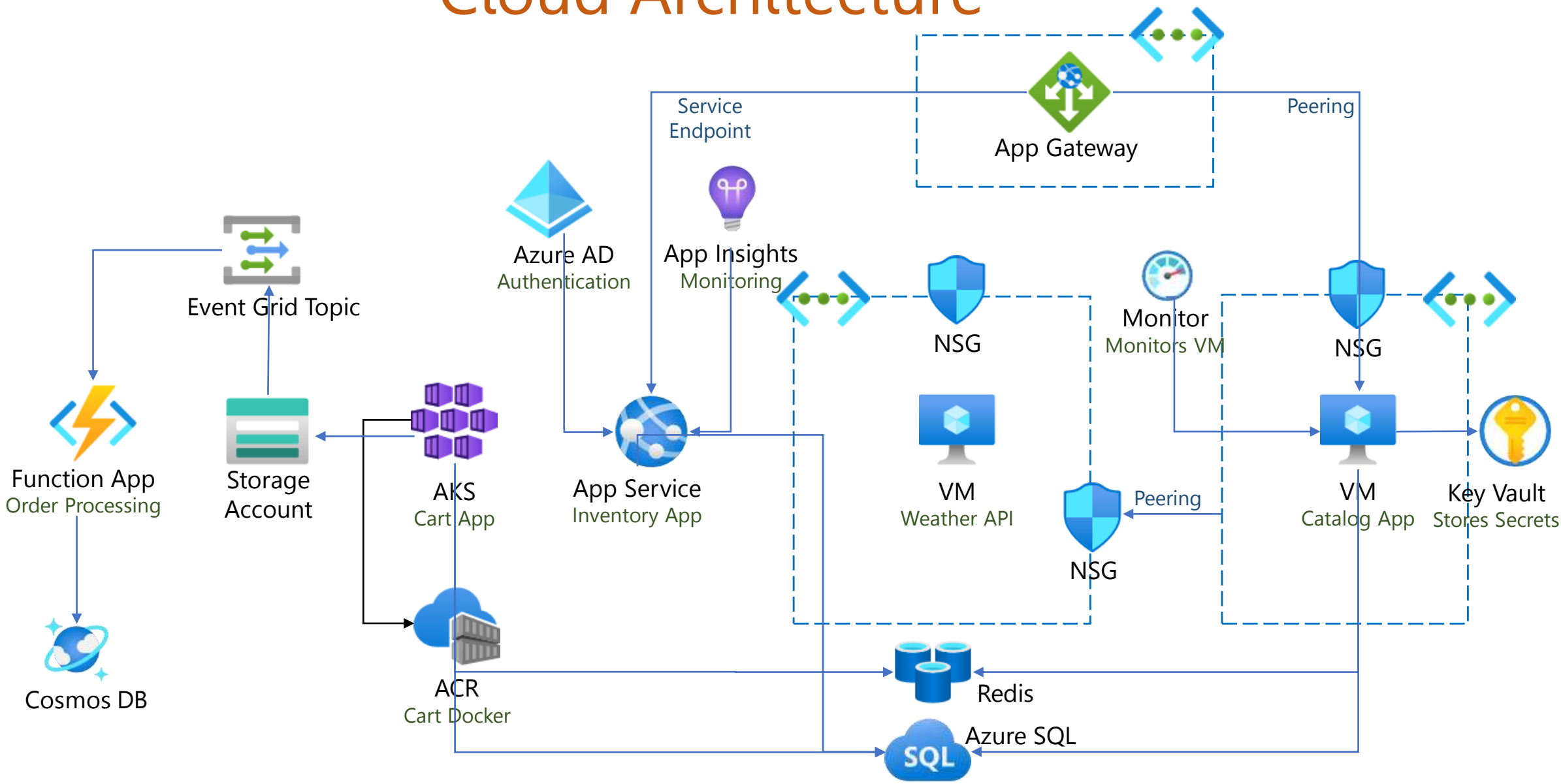
ReadIt!

Cloud Architecture



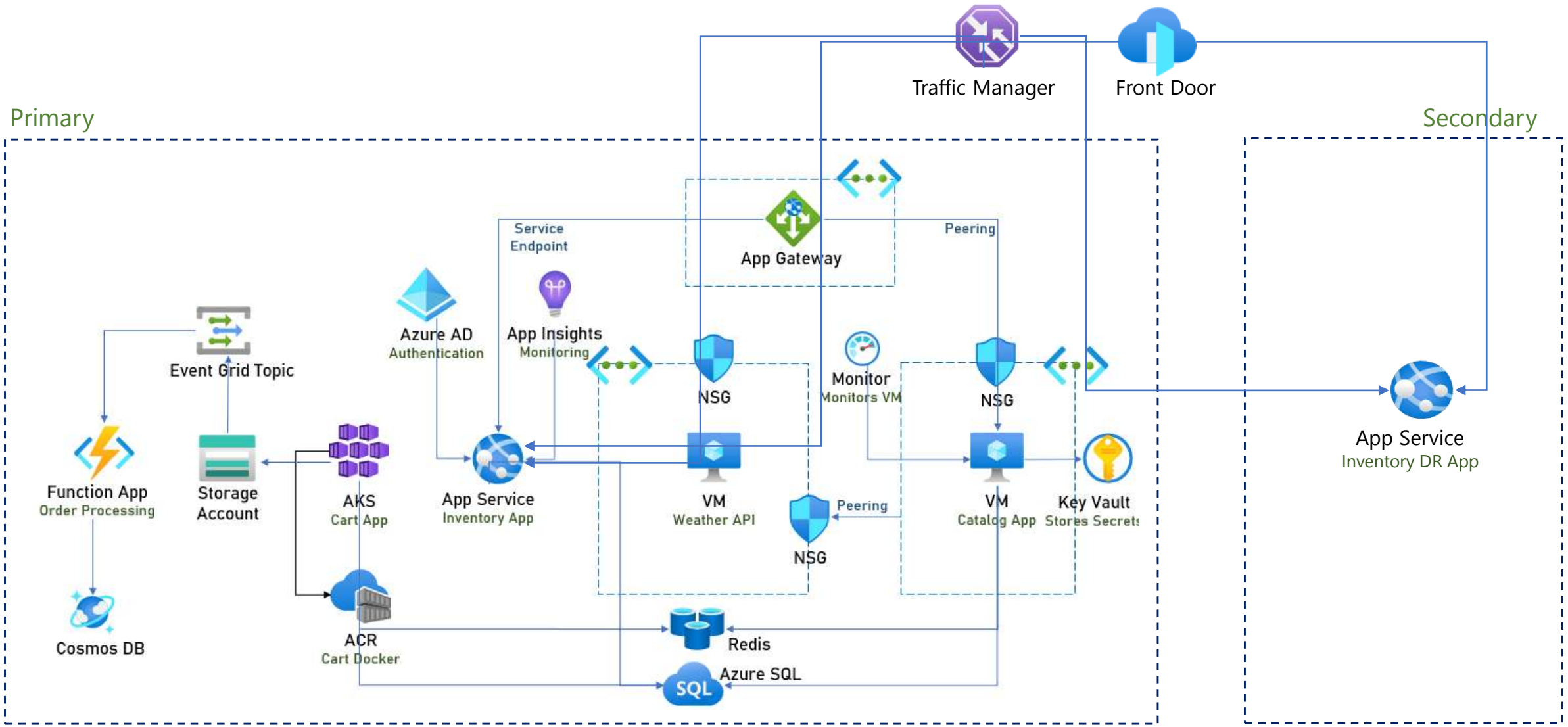
ReadIt!

Cloud Architecture



ReadIt!

Cloud Architecture with DR



Managing Costs in Azure

Memi Lavi
www.memilavi.com

Managing Costs in Azure

- Cost is one of the most important aspect of every cloud system
- Many decisions are made based on their cost impact
- Cost should be:
  - Transparent
  - Predictable
  - Monitored

Managing Costs in Azure

- Azure Cost Management is the central hub for all cost aspects
- Displays reports with sophisticated filters
- Makes predictions
- Enables alerts
- Can manage costs of resources outside Azure

Azure Policy

Memi Lavi
www.memilavi.com

Azure Policy

- Enforcing organizational standards and compliance at scale is not simple
- Quite important in the cloud
- Role-based access helps a little, but not enough

Azure Policy

- Examples:
  - All VMs should be built on a specific region
  - Only specific types of VM are allowed to be built
  - Tags must be specified on all resources in the resource group
  - App Services should only be accessible over HTTPS

Azure Policy

- Azure Policy is the mechanism for that
- It allows:
  - Defining policies
  - Assigning the policies to scopes (Subscription, Resource Group, specific resource)
- Is free (aside from auditing guest machines)

Azure Policy Evaluation

- Policies are evaluated:
  - When a resource is created / updated / deleted in a scope
  - When a new policy is assigned to a scope
  - When a policy is updated
  - Once every 24 hours (compliance evaluation cycle)

Azure Policy Outcome

- As a result of a non-compliant resource:
  - Resource change is denied
  - Resource change is logged
  - Resource is altered before the change
  - Resource is altered after the change
  - Related resources are deployed

Azure Policy Concepts

Definition → The policy definition: What is allowed, and to what resources (eg. Only specific VM sizes can be built)

Initiative → Logical grouping of definitions. (eg. VM definitions)

Assignment → Assigning the definition or initiative to a scope (Subscription, Resource Group, individual resource)

Effect → What is the outcome regarding non-compliant resource

Custom Policies

- So far we've used built-in policies
- You can create your own if there isn't one that satisfies your needs
- Look very closely at existing definitions and sample, you might find what you're looking for

Custom Policies Authoring

- Policy Definitions are JSON-based documents
- Describe the various properties of the policy, and the rule

Custom Policy Example

```
{
    "properties": {
        "displayName": "Deny storage accounts not using only HTTPS",
        "description": "Deny storage accounts not using only HTTPS. Checks the supportsHttpsTrafficOnly property on Sto
        "mode": "all",
        "parameters": {
            "effectType": {
                "type": "string",
                "defaultValue": "Deny",
                "allowedValues": [
                    "Deny",
                    "Disabled"
                ],
                "metadata": {
                    "displayName": "Effect",
                    "description": "Enable or disable the execution of the policy"
                }
            }
        },
        "policyRule": {
            "if": {
                "allOf": [
                    {
                        "field": "type",
                        "equals": "Microsoft.Storage/storageAccounts"
                    },
                    {
                        "field": "Microsoft.Storage/storageAccounts/supportsHttpsTrafficOnly",
                        "notEquals": "true"
                    }
                ]
            },
            "then": {
                "effect": "[parameters('effectType')]"
            }
        }
    }
}
```

Architecting Apps for Azure

Memi Lavi
www.memilavi.com

Architecting Apps for Azure

- Architecting for the cloud is different than classic Software Architecture
- Two main differences:
  - Use existing services
  - Consider cost

Use Existing Services

- Azure contains hundreds of services
- Whenever possible – use them
- Usually:
  - Managed
  - Reliable and Scalable
  - Cost effective

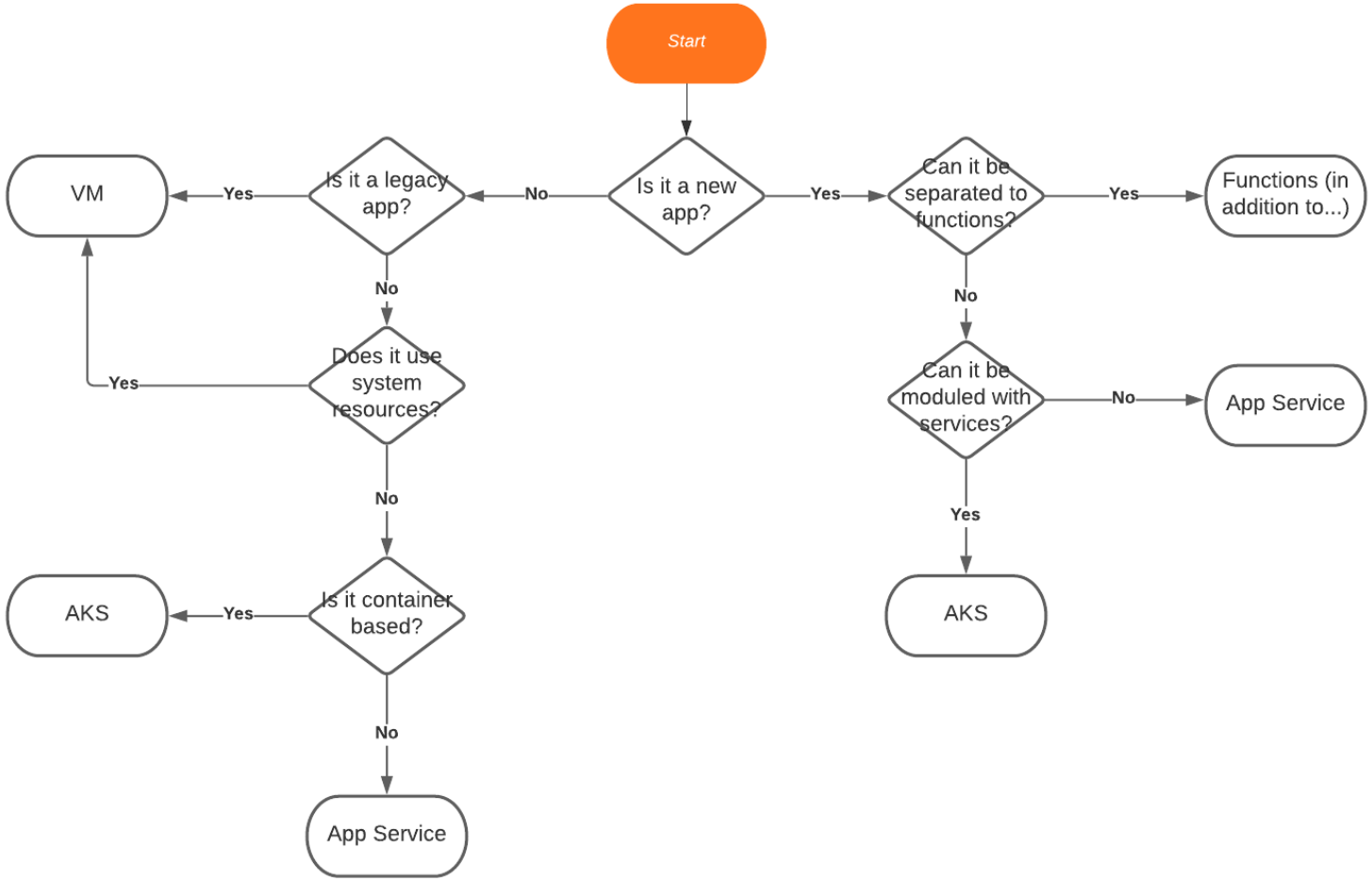
Consider Cost

- Cloud Architecture is cost oriented
- Always factor in the cost of the cloud service
- You'll sometimes go for limited service due to cost reasons
  - eg. Storage Queue vs Service Bus

Cloud Architecture

- In this section we'll review the various services we used and explain how to select the right one
- We'll discuss:
  - Compute
  - Data
  - Messaging
  - And some more…

Choosing Compute Platform



Choosing Data Platform

Data Type	Used For…	Examples	Options in Azure
Relational	Structured data	Items in store, demographic data	Azure SQL, MySQL, PostgreSQL
NoSQL	Semi-structured data	Reviews, Log records, when flexibility is required	Cosmos DB (with SQL, Mongo, Azure Table API)
Graph	Data representing relationships	Family tree	Cosmos DB (with Gremlin API)
Blob	Files, videos, docs	Items' photos	Azure Blob Storage

Choosing Messaging Platform

Service	Used For…	Guarantees Order	Max Msg Size	And also…
Storage Queue	Dead simple queueing	Yes	64KB	Extremely simple, no additional cost
Event Grid	Event driven architectures	No	1MB	Great integration with other services
Service Bus	Advanced queueing solutions	Yes	256KB	Advanced messaging features, durable
Event Hubs	Big data streaming	Yes	1MB	Low latency, designed for heavy load

Implementing Security

- Extremely important in the cloud
- Use the best practices discussed in the Security section
- Mainly:
  - Restrict access to VMs and App Services
  - Use NSG
  - Use encryption in data stores
  - Use strong authentication

Logging and Monitoring

- Azure offers various logging and monitoring tools
- Utilize alerts to notify on any exceptional situation
- Create dashboards to visualize the system state
- Use Application Insight to gain insights into your app

Azure Architecture Center

- Central hub for all-things Azure architecture
- How-tos, documents, design guidelines, case studies
- Fresh content, updated regularly

Azure Architecture Center

Guidance for architecting solutions on Azure using established patterns and practices.

ARCHITECTURE
Browse Azure architectures

CONCEPT
Explore cloud best practices

HOW-TO GUIDE
Assess, optimize, and review your workload

WHAT'S NEW
See what's new

Architecting Applications on Azure

Best practices and patterns for building applications on Microsoft Azure

https://docs.microsoft.com/en-us/azure/architecture

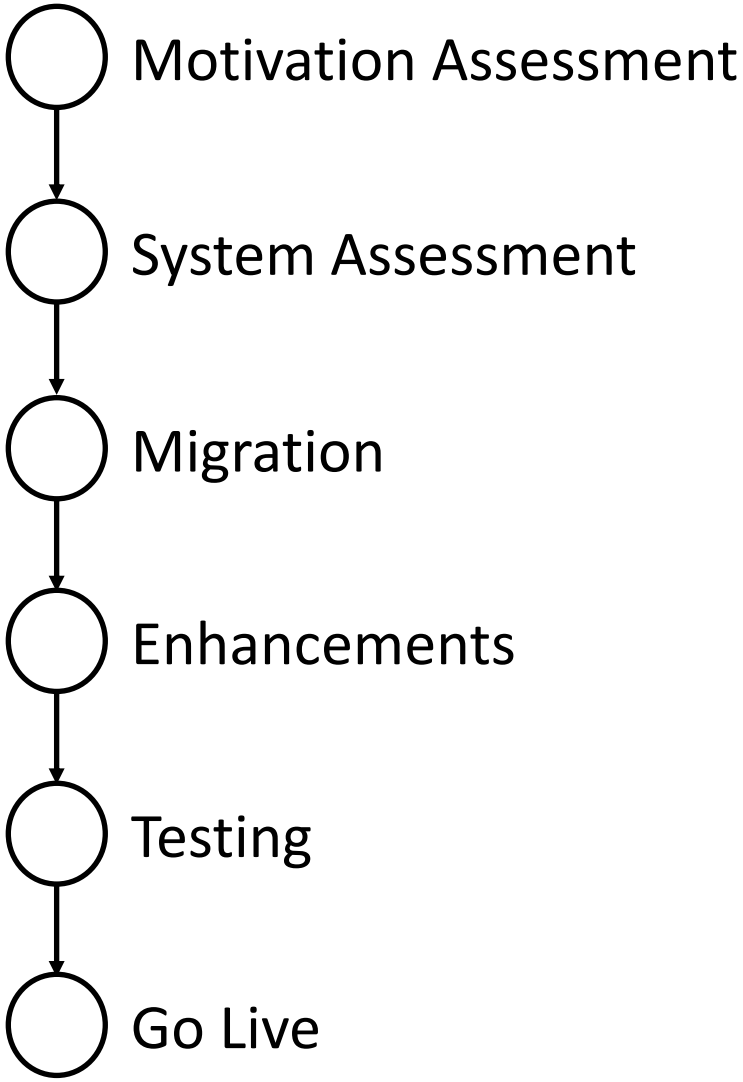
Migrating to Azure

Memi Lavi
www.memilavi.com

Migrating to Azure

- Many organizations want to migrate their apps to the cloud
- Various motivations
- Has to be planned ahead, and done methodically
- Rushing to the cloud could end up badly
- There's a well defined process that should be followed in order for the migration to complete successfully

The Migration Process



Motivation Assessment

- Answer the grand question:

Why?

(do we want to migrate to the cloud)

Possible Answers

- To save costs
- To take advantage of cloud capabilities (services, redundancy, scalability, etc)
- To modernize the system
- To attract new employees

Saving Costs

- Not always the case
- Sometimes cloud system can cost MORE than on-premises system
- CapEx vs OpEx
- A very thorough cost estimation should be conducted

Take Advantage of Cloud Capabilities

- Great motivation! (probably the best…)
- Make sure the migrated system can actually use cloud capabilities
- Example: Legacy, single-session app that cannot be scaled will end up on a single VM, just like on-prem

Modernize the System

- Usually, Modernization = Rewrite
- Why?
- Possible answers:
  - Not supported platforms
  - Difficult to hire employees
  - Licensing costs

Attract New Employees

- Not a very good motivation, but it works…
- The organization has to be part of the cloud trend in order to attract new employees

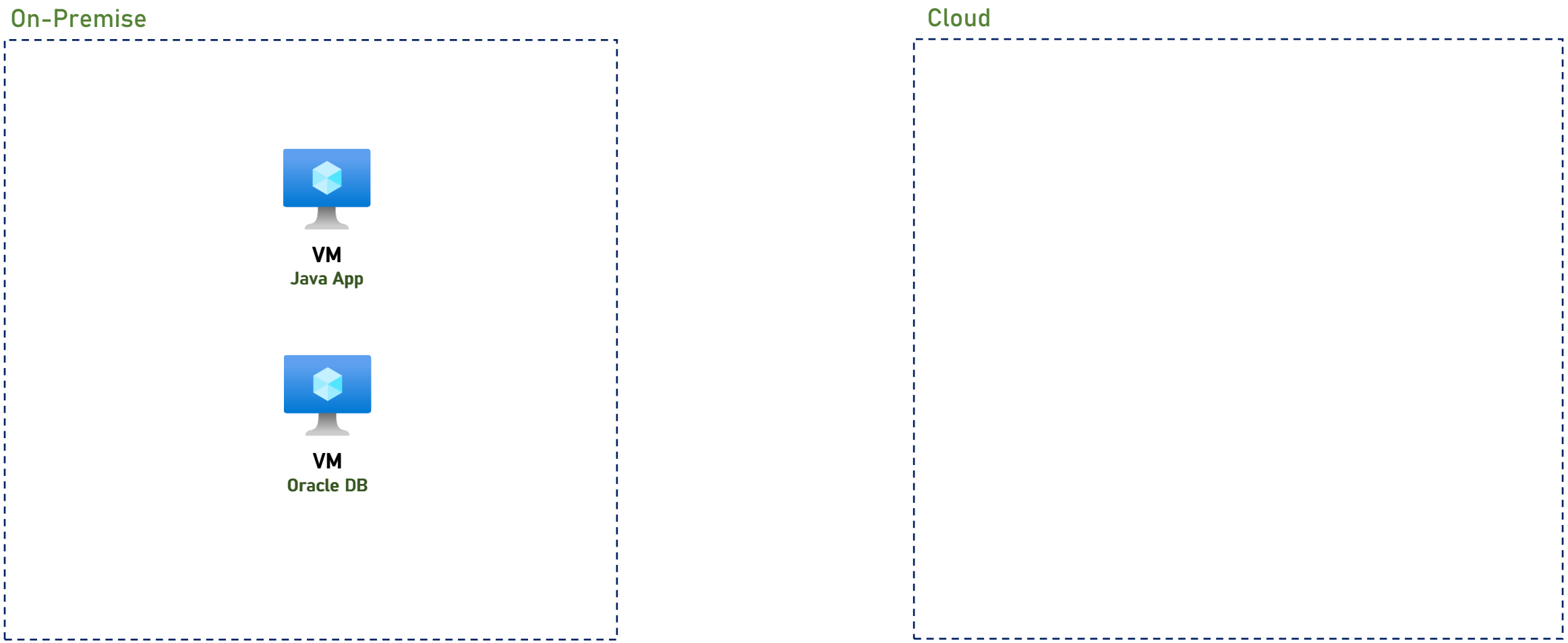
Migration Strategies

Lift & Shift → Install the app in the cloud “as-is”, without any changes, usually on a VM

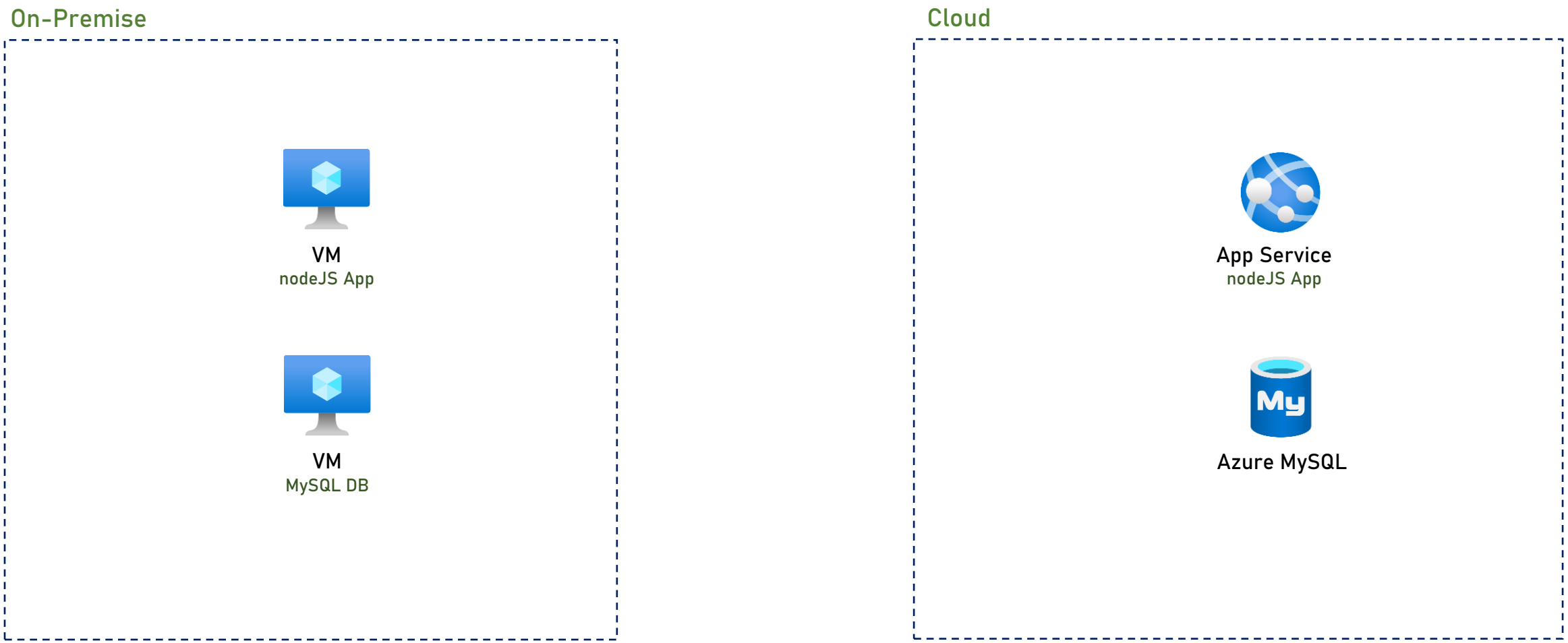
Refactoring → Modify the app a bit so it can run on managed services (ie. App Services)

Rewrite → Rewrite the app from scratch, usually in a modern platform, and take advantage of all cloud services

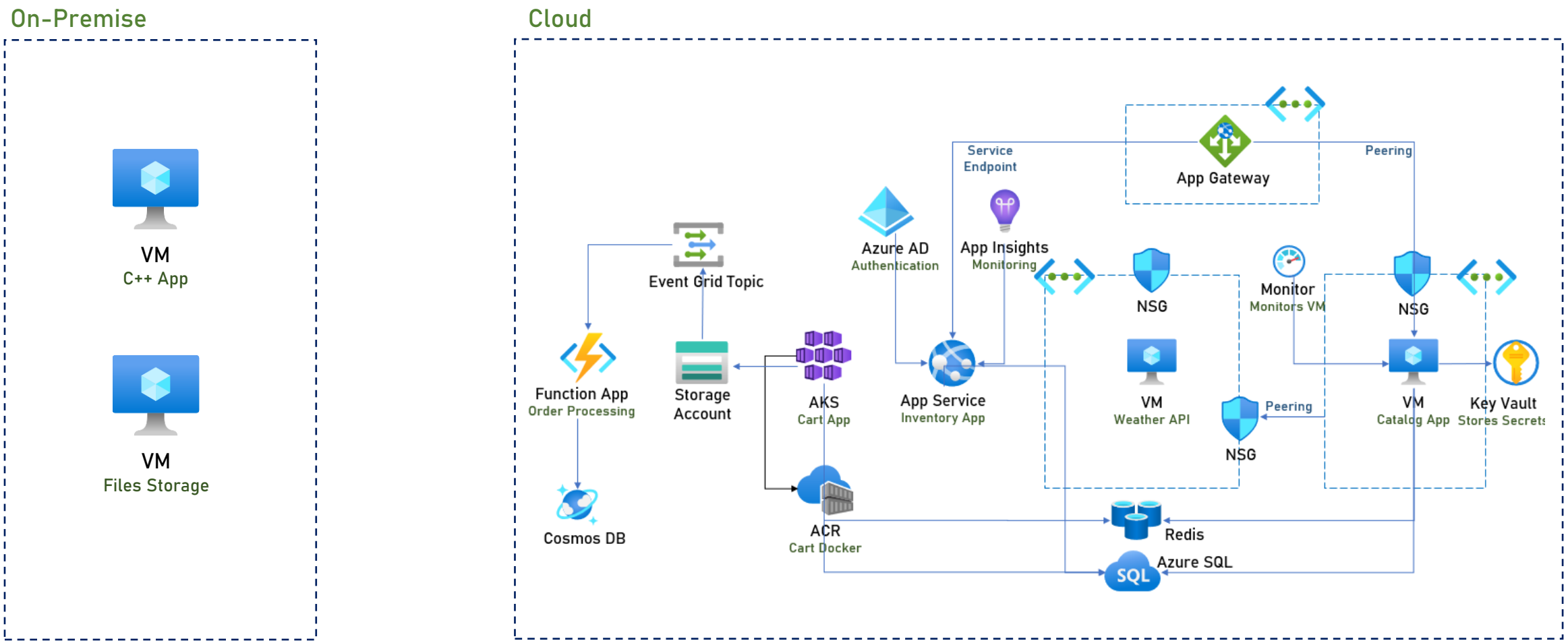
Lift & Shift



Refactor


On-Premise
VM
nodeJS App
VM
MySQL DB
Cloud
App Service
nodeJS App
Azure MySQL

Rewrite


On-Premise
VM
C++ App
VM
Files Storage
Cloud
Service
Endpoint
App Gateway
Peering
Azure AD
Authentication
App Insights
Monitoring
Event Grid Topic
NSG
Monitor
Monitors VM
NSG
Function App
Order Processing
Storage
Account
AKS
Cart App
App Service
Inventory App
VM
Weather API
Peering
NSG
VM
Catalog App
Key Vault
Stores Secrets
Cosmos DB
ACR
Cart Docker
Redis
Azure SQL
SQL

Comparing Cloud Migration Strategies

System Assessment

- Goal:
  - To find out what is the best way to migrate the system to the cloud
  - Doing this by asking the right questions

System Assessment

- Questions we need to ask:

What is the runtime platform of the system and on which OS? (.NET, Java, C++ etc.)

How is it deployed today? (VM, Docker…)

What database(s) is used?

What is the authentication mechanism?

Any interfaces to organizational systems?

Any work with hardware? (dongles…)

System Assessment

- Answers dictate migration strategy, if possible at all:

What is the runtime platform of the system and on which OS? (.NET, Java, C++ etc.)

→

If C++, Refactor is not an option

What is the authentication mechanism?

How is it deployed today? (VM, Docker…)

Any interfaces to organizational systems?

What database(s) is used?

Any work with hardware? (dongles…)

System Assessment

- Answers dictate migration strategy, if possible at all:

What is the runtime platform of the system and on which OS? (.NET, Java, C++ etc.)

What is the authentication mechanism?

How is it deployed today? (VM, Docker…)

If yes, perhaps containerization is not an option

Any interfaces to organizational systems?

What database(s) is used?

Any work with hardware? (dongles…)

System Assessment

- Answers dictate migration strategy, if possible at all:

What is the runtime platform of the system and on which OS? (.NET, Java, C++ etc.)

What is the authentication mechanism?

How is it deployed today? (VM, Docker…)

Any interfaces to organizational systems?

What database(s) is used?

Any work with hardware? (dongles…)

Azure Migrate

- A central hub for assessing and migrating various resources
- Uses platform-specific agents to discover the resources that can be migrated
- Provides migration recommendations
- Free

Azure Migrate

Microsoft Azure

Search resources, services, and docs (G+/)

Home >

Azure Migrate

Microsoft

Search (Ctrl+/)

Get started | Explore more

- Overview

Migration goals

- Servers
- Databases
- VDI
- Web Apps
- Data Box

Manage

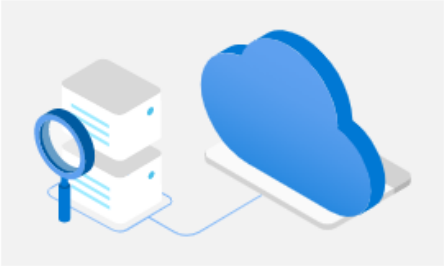
- Discovered items

Support + troubleshooting

- New support request

Migrate your on-premises datacenter to Azure

Discover, assess and migrate your on-premises applications using Microsoft or third-party tools, or find an expert to help with your migration. Learn more



Windows and Linux servers

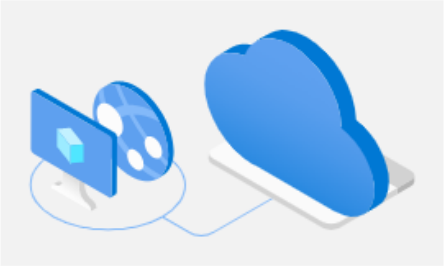
Discover, assess and migrate your on-premises VMware and Hyper-V virtual machines or Physical servers to Azure.

Assess and migrate servers

SQL and other databases

Assess and migrate your on-premises databases to Azure SQL Database Managed Instance or Azure SQL Database.

Assess and migrate databases



Explore more scenarios

Assess and migrate web apps, migrate data and assess virtual desktop infrastructure (VDI). Find giudence on various migration activites

Explore more

Azure Migrate

- Good for low-level assessment (platforms used etc.) but won't deal with other considerations
  - ie. Interfaces with organizational systems
- Can be used as a first-step, but must perform manual assessment afterwards

Migration

- Time for actual migration…
- Migration strategy depends on the system assessment results

Lift & Shift

- The easiest strategy
- Simply create VM images and build new VMs in the cloud
- Don't forget to put VMs in appropriate VNet and define NSG

Refactor

- Should be done in two phases:
  - Lift & Shift – Make sure the app works in the cloud as-is
  - Refactor – gradually improve the system and integrate cloud services
- Don't try shortcuts!

Rewrite

- Not really a migration…
- Design the system from the ground up to be cloud native
- Use as many cloud services as possible

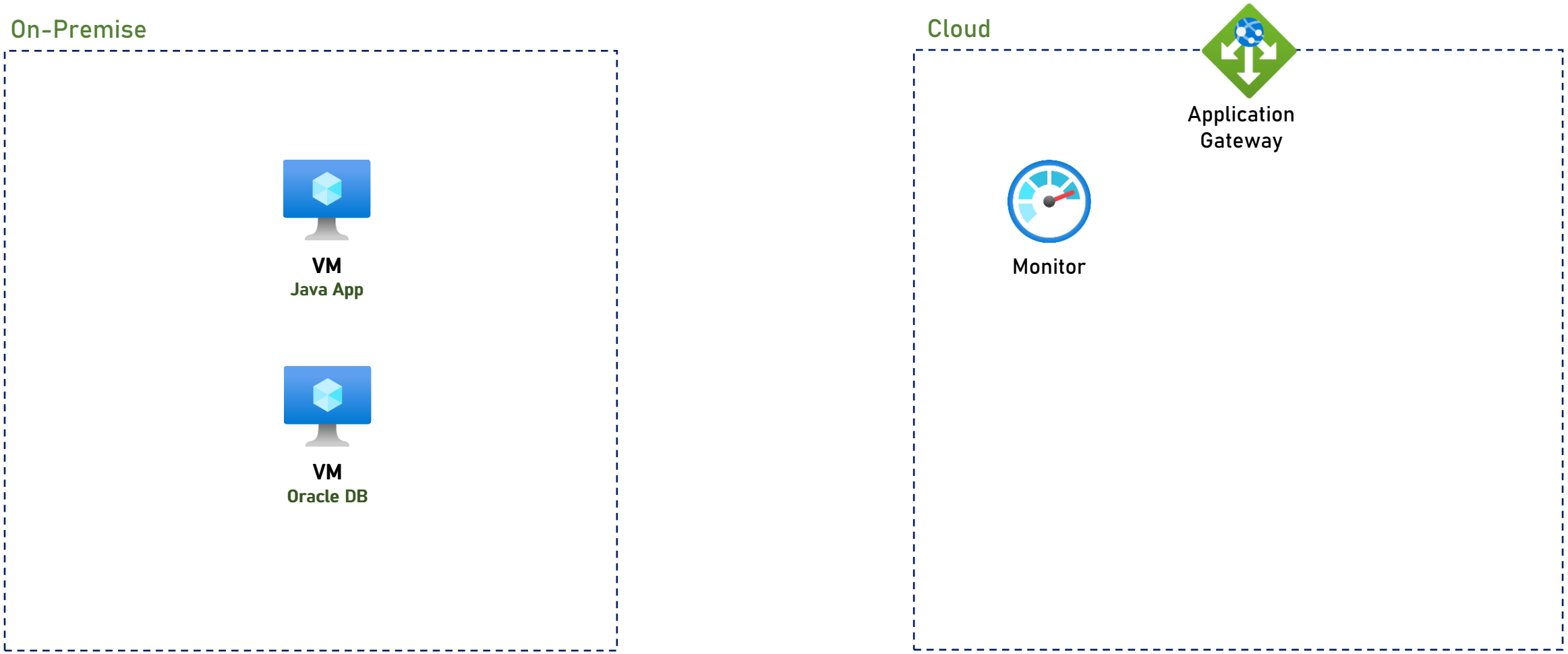
DB Migration

- In general:
  - Prefer the managed version of the DB (and not on a VM)
  - Migration is better done using the DB's own tools and not via Azure migration services

App Enhancements

- After migration, enhance the system
- Not necessarily requires code changes
- Main areas for improvements:
  - Logging and Monitoring using Azure Monitor
  - Network protection using Application Gateway

Lift & Shift Example



Testing

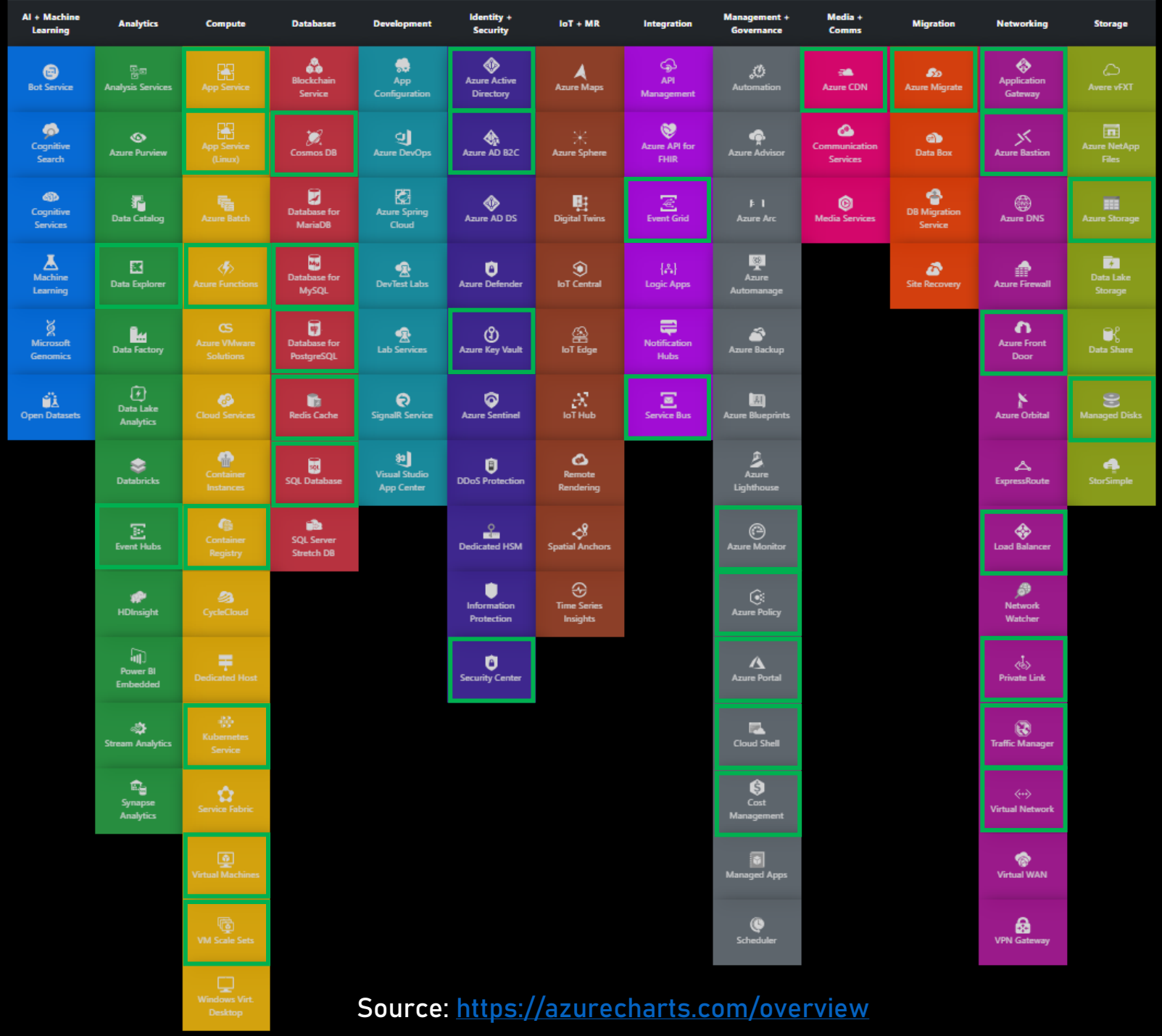
- Testing in cloud is similar to on-prem
- Put strong emphasis on logging and monitoring
- Make sure you have access to system's data
- If system is auto-scaled or DRed – test these scenarios
- Check performance – might vary from the on-prem figures

Go Live

- Congratulations!
- Keep an eye on the costs
  - Set up budget alerts
  - Define tags
  - Look at the data at least once a month

Advanced Services

Memi Lavi
www.memilavi.com

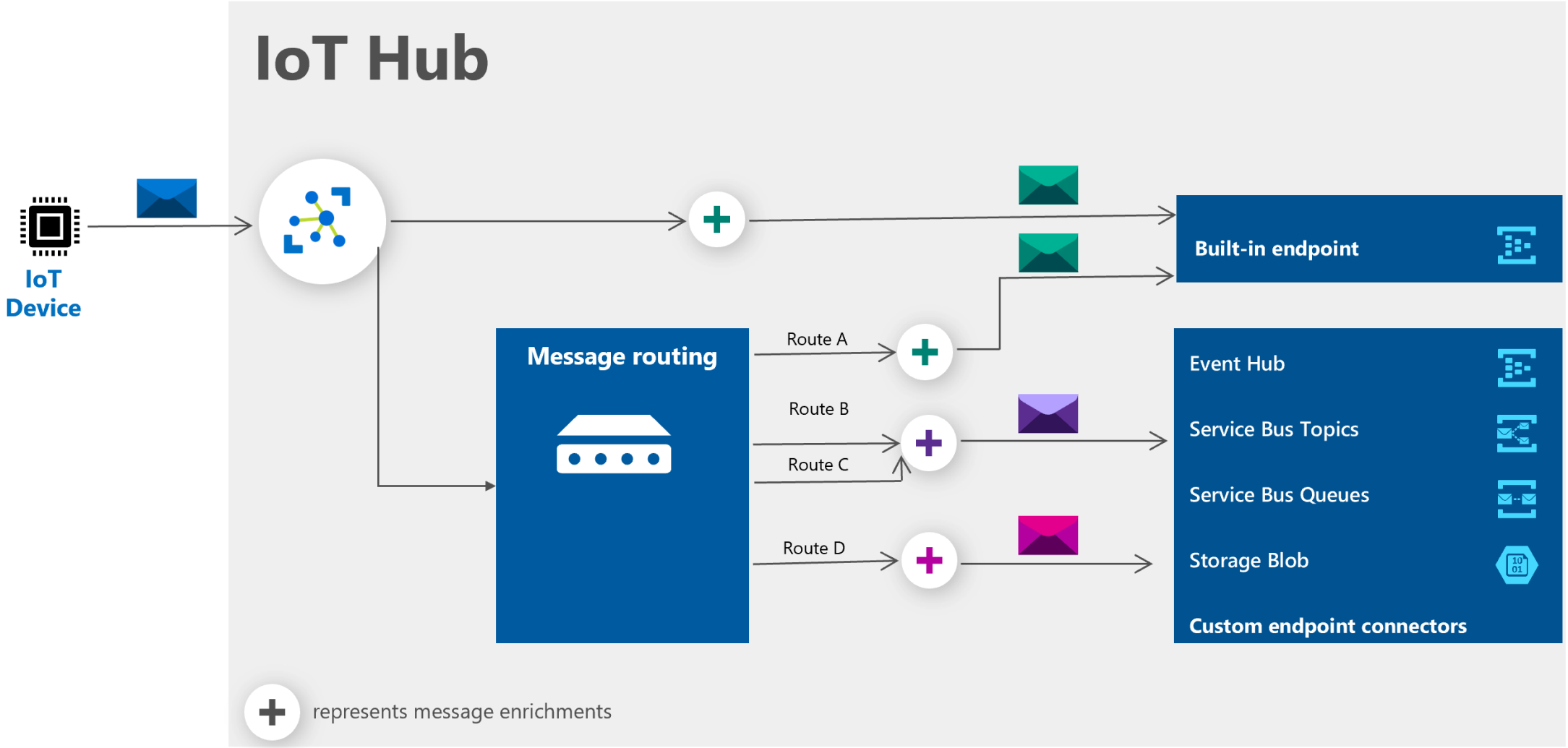


Source: https://azurecharts.com/overview

IOT Hub

- Central message hub for IoT devices
  - IoT = Internet of Things (cameras, sensors, connected cars etc.)
- Handles security, reliability, enrichment, routing and more
- Integrates with other Azure services
- Handles millions of devices easily

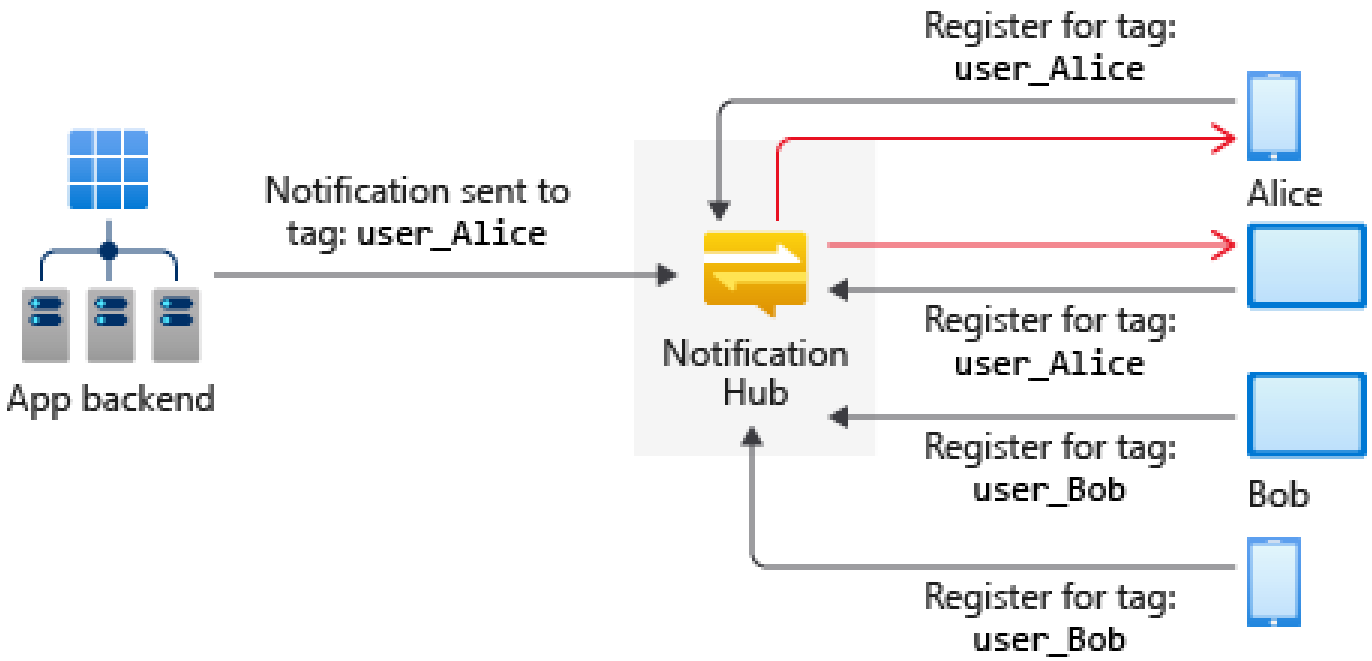
IOT Hub


IoT Hub
IoT Device
Built-in endpoint
Message routing
Route A
Route B
Route C
Route D
Event Hub
Service Bus Topics
Service Bus Queues
Storage Blob
Custom endpoint connectors
represents message enrichments

Notification Hub

- Central hub for sending push notifications to any platform
- Supports iOS, Android, Windows, Kindle and Baidu
- Can be used by any backend, including on-premise one
- Supports million of mobile devices

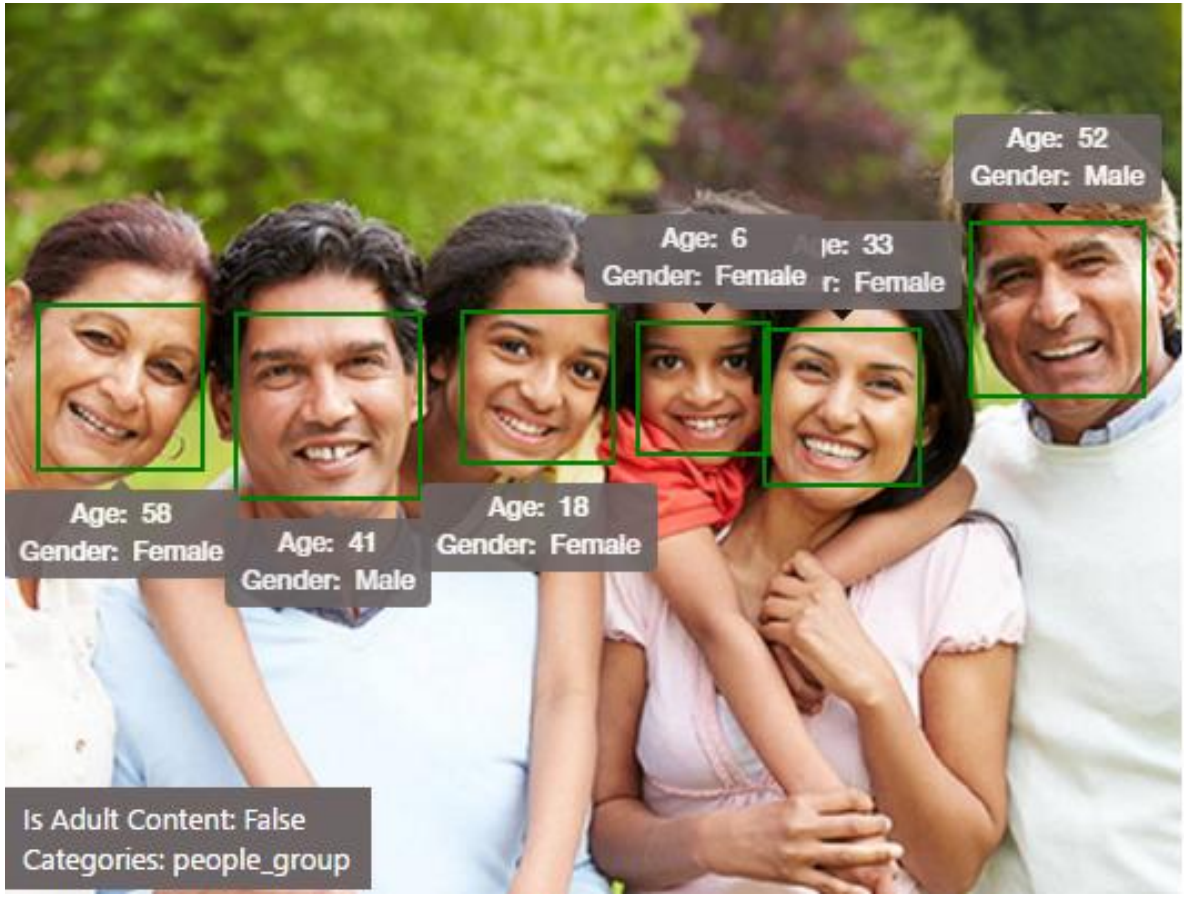
Notification Hub



Cognitive Services

- Set of APIs running AI (Artificial Intelligence) algorithms
- Does not require machine learning knowledge
- Enables: Anomaly detection, Language Understanding, Translator, Speech to Text, Computer Vision and lots and lots more…
- Extremely easy to use

Cognitive Services



Summary

- Azure has hundreds of services
- Before developing your own – check if it doesn't already exist
- We'll cover many of them in future courses ☺

Microsoft Azure

From Zero to Hero – The Complete Guide

Architecture Summary

When designing cloud architectures for Microsoft Azure, use this summary that will help you design the system select the right resources for the right task.

Area	Resources / Notes
Compute	Virtual Machines (VMs) – When a full control is needed, or dev platform is not supported on any other cloud service (e.g. C++). Can be auto scaled using Scale Set. App Service – PaaS for web apps. Use when system is a web app running on modern platform. Not requiring any setup or configuration. Great integration with authentication providers and Application Gateway. Azure Kubernetes Services (AKS) – If your apps already run on Kubernetes or Docker containers – use it. If you plan to deploy your app using containers – use it.

	Azure Functions – Use for focused, lightweight actions (calculations, conversions, validation etc.). Extremely efficient, beware of cold starts.
Networking	VNet – Virtual Network. By default inaccessible to other VNets. Design your app around VNets using the Hob-and-Spoke model. Subnet – Logical segment inside a VNet. By default accessible from other subnets in the VNet. Network Security Group (NSG) – Filters traffic based on 5 tuples. ALWAYS set up NSG in front of every subnet. Load Balancer – Balances load across various resources based on various algorithms. Works on Layer 4. Use ONLY for internal resources. Application Gateway – Used to expose web endpoint to the outside world. Load balancer, WAF (optional), works on Layer 7. Use in front of App Services.
Data	Relational Databases – Azure SQL (the only resource with 99.995% SLA), Azure MySQL, Azure Postgres NoSQL Database – Cosmos DB (the only resource with 99.999% SLA) Object Store – Blob Storage

Messaging	Storage Queue – Dead simple queueing, no additional cost, max msg size – 64KB Event Grid – Messaging system for Event Driven Architectures, great integration with other services, max msg size – 1MB Service Bus – Advanced queueing solution with advanced features, durable, max msg size – 256KB Event Hubs – Big data streaming, designed for heavy load, Kafka-based. Max msg size – 1MB
Authentication	Azure Active Directory – Identity and Access Manager (IAM), extremely robust, supports MFA, conditional access and more. Great integration with App Services. Azure AD B2C – Simplifies integration with apps for identity scenarios (log in, log out, sign up, etc)
Monitoring	Set up Alerts to get notifications when something goes wrong Use Metrics to see system's status Read Logs to find out what the system did Put important information on Dashboards to get wholistic view Use Tags to categorize the resources

Security	- Close unnecessary open ports of a VM - Use NSG - Use authentication - Encrypt data at rest and at transit - Use KeyVault to securely store secrets - Use Security Center regularly
DR	- Decide between hot and cold DR - Remember – hot DR is much more difficult to design and expensive to implement - Use Traffic Manager or Front Door for automatic routing

I Hope you enjoyed the course, and that it made you a Microsoft Azure expert. Stay tuned to more courses on Azure, which will make you an even better Azure Architect!

For any question or comment contact me at:

memi@memilavi.com

Thanks,

Memi

Download the Azure Architecture Summary

Memi Lavi
www.memilavi.com

Azure Architecture Summary

- A great reminder of the various aspects of the cloud services
  - Compute, Networking, Data, Messaging etc.
- Outlines the various alternatives of every aspect
- Extremely handy during the design process

Azure Architecture Summary

Download the Azure Architecture Summary from the resources!

The ultimate, practical guide to help you design great Azure apps!

What We've Learned

- What is the cloud
- Using Azure services
- Compute, Data, Networking, Messaging, Identity and lots more
- Hands On! Hands On! Hands On!
- How to become a great Azure Developer & Architect!

ReadIt!

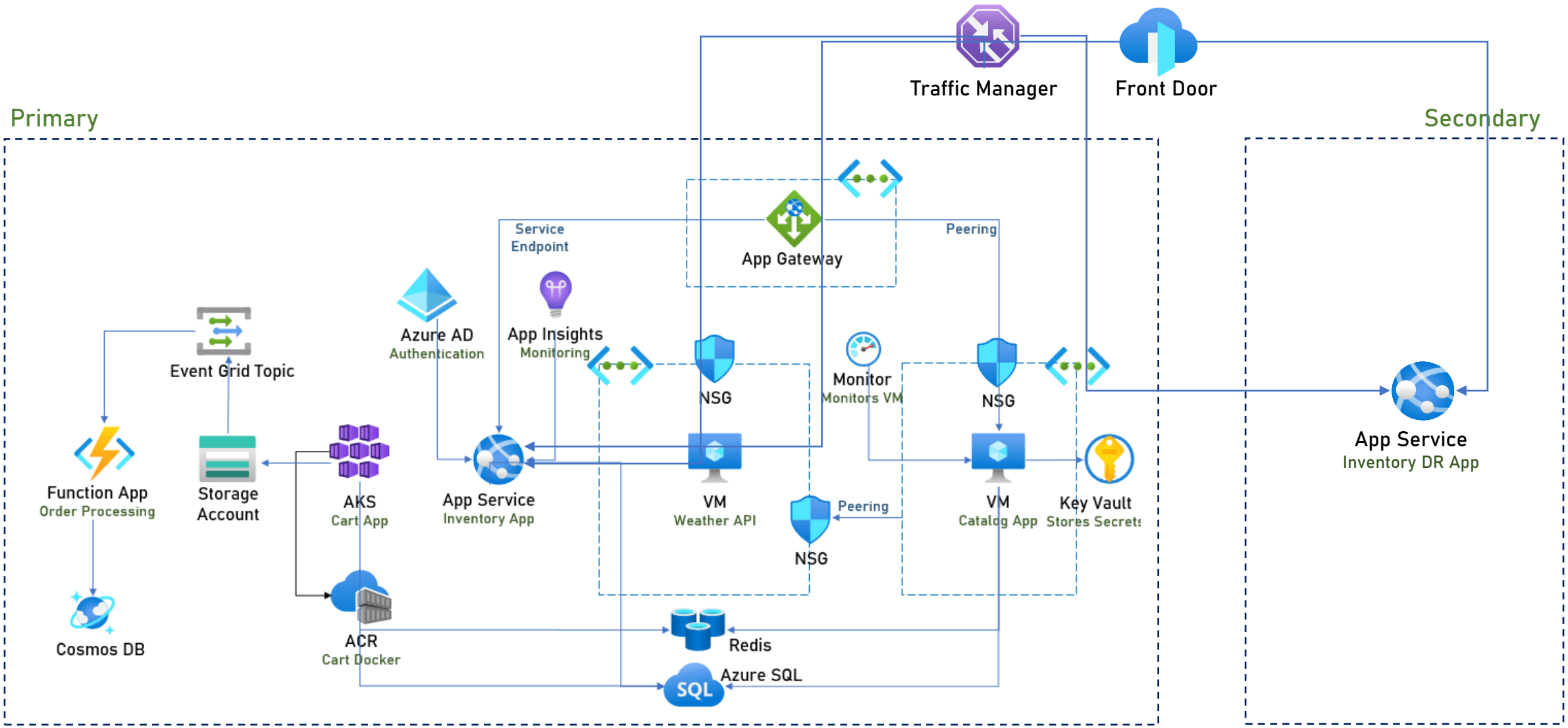
Cloud Architecture

VM
Weather API

VM
Catalog App

ReadIt!

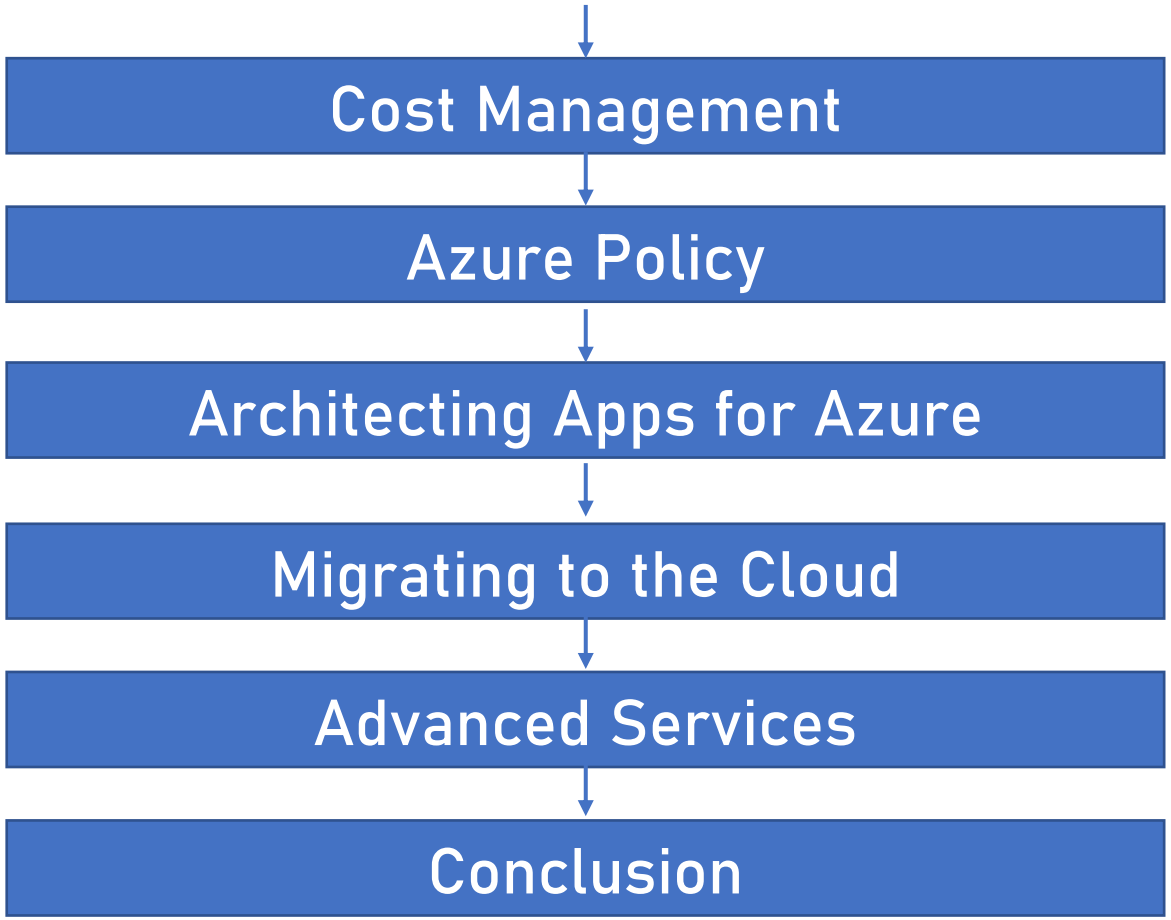
Cloud Architecture



Agenda

- Welcome
- Introduction to the Cloud
- Introduction to Azure
- First Look at Azure
- Basic Concepts
- Introducing Our App
- Compute
- Networking
- Data
- Messaging
- Azure Active Directory
- Monitoring
- Security
- DR

Agenda


Cost Management
Azure Policy
Architecting Apps for Azure
Migrating to the Cloud
Advanced Services
Conclusion

Thanks!